AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ACTION THROUGH INNOVATION: PRIVATE SECTOR SOLUTIONS TO RECOUPING STOLEN PANDEMIC LOAN FUNDS

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

HEARING HELD
SEPTEMBER 27, 2023



Small Business Committee Document Number 118–027
Available via the GPO Website: www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
53–334 WASHINGTON : 2024

HOUSE COMMITTEE ON SMALL BUSINESS

ROGER WILLIAMS, Texas, *Chairman*
BLAINE LUETKEMEYER, Missouri
PETE STAUBER, Minnesota
DAN MEUSER, Pennsylvania
BETH VAN DUYNE, Texas
MARIA SALAZAR, Florida
TRACEY MANN, Kansas
JAKE ELLZEY, Texas
MARC MOLINARO, New York
MARK ALFORD, Missouri
ELI CRANE, Arizona
AARON BEAN, Florida
WESLEY HUNT, Texas
NICK LALOTA, New York
NYDIA VELÁZQUEZ, New York, *Ranking Member*
JARED GOLDEN, Maine
KWEISI MFUME, Maryland
DEAN PHILLIPS, Minnesota
GREG LANDSMAN, Ohio
MORGAN MCGARVEY, Kentucky
MARIE GLUESENKAMP PEREZ, Washington
HILLARY SCHOLTEN, Michigan
SHRI THANEDAR, Michigan
JUDY CHU, California
SHARICE DAVIDS, Kansas
CHRIS PAPPAS, New Hampshire

BEN JOHNSON, *Majority Staff Director*
MELISSA JUNG, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Hon. Roger Williams	1
Hon. Nydia Velázquez	2

WITNESSES

Mr. Richard C. Breeden, Chairman, Breeden Capital Management, LLC, Lantana, FL	5
Mr. JT Taylor, Senior Director of Fraud Investigations and Operations, ID.me, Mclean, VA	6
Mr. Dean Zerbe, National Managing Director, Alliantgroup, Washington, DC	8
Ms. Linda Miller, Former Deputy Executive Director, PRAC, Currently Chief Executive Officer of Audient Group, LLC, Washington, DC	10

APPENDIX

Prepared Statements:	
Mr. Richard C. Breeden, Chairman, Breeden Capital Management, LLC, Lantana, FL	33
Mr. JT Taylor, Senior Director of Fraud Investigations and Operations, ID.me, Mclean, VA	46
Mr. Dean Zerbe, National Managing Director, Alliantgroup, Washington, DC	68
Ms. Linda Miller, Former Deputy Executive Director, PRAC, Currently Chief Executive Officer of Audient Group, LLC, Washington, D	82
Questions and Answers for the Record:	
Questions from Hon. Velázquez to Ms. Linda Miller and Answers from Ms. Linda Miller	86
Additional Material for the Record:	
Discussion Draft	88

ACTION THROUGH INNOVATION: PRIVATE SECTOR SOLUTIONS TO RECOUPING STOLEN PANDEMIC FUNDS

WEDNESDAY, SEPTEMBER 27, 2023

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 9:58 a.m., in Room 2360, Rayburn House Office Building, Hon. Roger Williams [chairman of the Committee] presiding.

Present: Representatives Williams, Stauber, Meuser, Salazar, Molinaro, Alford, Bean, LaLota, Velázquez, Phillips, McGarvey, Gluesenkamp Perez, Scholten, Chu, and Davids.

.

Chairman WILLIAMS. Good morning. Before we get started I want to recognize our colleague from the great state of Missouri for the prayer and the pledge.

Would you please stand?

Mr. ALFORD. Let's go to God in prayer.

God, we are just so thankful to be here today on this Small Business Committee. We ask a blessing on our Chair and our Ranking Member that they will guide us and direct us as we question the witnesses today and give us discernment and wisdom, God, that you will help us with our votes to lead this great nation to greater prosperity through small business, the fabric of America, God. Through Jesus Christ I pray. Amen.

I pledge allegiance to the flag of the United States of America. And to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

Chairman WILLIAMS. Good morning, everyone. And I now call the Committee on Small Business to order.

Without objection, the Chair is authorized to declare a recess of the Committee at any time.

I now recognize myself for my opening statement.

Welcome to today's hearing where we will be looking at the unacceptable amount of fraud that occurred during the COVID-19 pandemic and what could be done to recoup those stolen taxpayer dollars.

During the pandemic, the SBA took an outsized role in helping America's economy. The PPP and the EIDL loan programs were incredibly important for our nation's entrepreneurs and allowed many businesses to keep their doors open throughout all the uncertainty.

However, the after action reports show that these programs were extremely susceptible to fraud. The OIG estimates that $200 billion dollars in taxpayers' money were given out to bad actors which accounts for almost 20 percent of all pandemic lending. This is completely unacceptable and we must find ways to rectify these issues.

If we keep doing business as normal, the OIG says that they will have more than 100 years of casework to go through in order to properly investigate all the loans that have been tagged as fraudulent. In the private sector, if there was an accounting hole of this magnitude, the business owners would do all they could to get his receivable back into the bank account. This Commitmtee is working to find creative solutions to do just that and recoup the stolen pandemic funds for the taxpayers.

I am proud that in our last two markups, this Committee passed four COVID fraud bills that must be done to recover those stolen dollars. We cannot allow the American taxpayer to be on the hook for 200 billion, and we must do a better job to maintain public trust that this level of fraud was an isolated event.

I look forward to discussing with our witnesses' innovative ideas on how to catch fraud early and ensure hard-earned taxpayer dollars are being used for their intended purpose. This could mean greater use of data matching tools and proving interagency collaboration or mandating more strict standards for identity verification in any program that gives out taxpayer dollars.

Additionally, we must find a better way to recover stolen funds on the back end. There will always be fraudsters and criminals looking to take advantage of any government program that is giving our money but we must have the ability to catch these bad actors and bring them to justice so they will not be able to continue defrauding the American people. Regardless of what solutions are brought to the table, it is clear we cannot continue with business as usual.

Too many times in government we hear that something can't be done or that isn't how it was done in the past. Well, the private sector does not think like this. They encounter a problem; they immediately go to work and then they fix it.

I am excited to hear from our witnesses today on new ways we can work to prevent and detect fraud moving forward. I thank all our witnesses for being here, and I look forward to this discussion.

With that I will now yield to the distinguished Ranking Member from New York, Ms. Velázquez.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

We are here today to discuss the SBA's efforts in recovering fraudulent loans and preventing future fraud. Over the past 3 years, this Committee has played an integral role in examining the pandemic relief programs which helped millions of small businesses stay afloat in unprecedented times. Approximately $1.2 trillion of economic aid was dispersed through SBA's pandemic relief programs over the course of the pandemic, with much of that originating in the first 9 months of the pandemic under the Trump administration.

While there may be disagreement on the actual estimates of fraud, it is clear we need to work together to protect the integrity of SBA programs from bad actors. The SBA under the leadership

of Administrator Guzman has taken strong steps to root out fraud in the pandemic relief programs and put strong controls in place to prevent future fraud.

Earlier this year we heard testimony from Administrator Guzman that SBA is doing just that. In 2022, SBA established a Fraud Risk Management Board aligning its practices with GAO's oversight policies. A new role was also created-the SBA's Special Counsel for Enterprise Risk to advise the Administrator on fraud and risk management activities. The agency continues to work collaboratively with the SBA Inspector General, the interagency COVID-19 Fraud Enforcement Task Force, and the Department of Justice to recover stolen funds.

With that said, we must be clear. The SBA is not an investigative agency, and it does not have a team of auditors, investigators and attorneys, or state-of-the-art data analytics technology to root out and prosecute fraud. That is the role of the Inspector General. It is important that we understand the difference between the missions of the SBA and the Office of the Inspector General if we are going to effectively develop policies to prevent and recover fraud.

To that end, the single, most important action we can take to combat fraud is to fully fund the Inspector General's budget request. Unfortunately, their budget for fiscal year 2024 was slashed from 47.7 million to 32 million in the House Financial Services and General Government Appropriations Bill. We are just days away from a government shutdown which will limit the OIG's and law enforcement efforts to recover fraudulent funds. Put simply, this is unacceptable. We must take our responsibilities seriously.

In the last Congress, I joined with Representative Luetkemeyer to sponsor legislation to extend the statute of limitations for fraud in PPP and EIDL to 10 years. These two bills which became law sent a strong message that unscrupulous behavior would not be tolerated and that those who commit fraud will be held accountable in the years to come—but it is all for not if we do not give the Inspector General the resources it needs.

I look forward to hearing from our witnesses today, and I am certainly open to new, creative ideas provided we are committed to fully funding the Office of the Inspector General and the law enforcement community.

Thank you, Mr. Chairman. I yield back.

Chairman WILLIAMS. Thank you very much.

And I will now introduce our witnesses.

The first witness here with us today is Mr. Richard Breeden. Mr. Breeden is the Chairman of Breeden Capital Management, LLC, located in Greenwich, Connecticut. Mr. Breeden founded Breeden Capital Management in 2005 focused on taking concentrated investment stakes in mid-cap companies and supporting staffs to improve shareholder value. In addition to serving as the Chairman of Breeden Capital Management, he also serves as Chairman of the Nominating and Governance Committee of the Board of Steris PLC and is a trustee of the George H. W. Bush Presidential Library. Prior to starting his company, Mr. Breeden served as the 24th Chairman of the U.S. Securities and Exchange Commission, as well as several positions under Presidents Reagan, Bush, and Clinton. Mr. Breeden attended Stanford University where he received his

B.A. and went on to attend Harvard Law School where he earned his J.D.

Mr. Breeden, thank you for being with us today, and we look forward to the conversation that is ahead with you.

Our next witness with us today is Mr. JT Taylor. Mr. Taylor is a senior director of Fraud Investigations and Operations at ID.me located in McLean, Virginia. ID.me allow individuals to securely verify their identity online, helping to prevent fraud and abuse. Prior to his time at ID.me, Mr. Taylor worked for the U.S. Secret Service as a special agent, as a supervisory intelligence operations officer for the Office of the Director of National Intelligence, and as an intelligence officer for the U.S. Navy. Mr. Taylor went to West Virginia. They play TCU this Saturday. I did not know if you knew that or not. Where he earned his bachelor of science in management information systems, as well as Norwich University where he earned his master of science, and Louisiana State University where he earned his master of business administration.

Mr. Taylor, thank you for joining us today, and we look forward to our conversation.

The next witness with us today is Mr. Dean Zerbe. Mr. Zerbe is the national managing director of Alliantgroup located in Houston, Texas. At Alliantgroup, Mr. Zerbe is responsible for monitoring tax-related legislative activities here in Washington to keep clients and staff informed and help direct Alliantgroup service offerings to ensure client needs are met. Prior to his time at Alliantgroup, Mr. Zerbe was senior counsel and tax counsel to the Senate Committee on Finance where he worked with the Chairman of the Finance Committee, Senator Grassley on tax legislation. During this time on the Finance Committee, he was involved with almost every piece of tax legislation signed into law including the 2001 and 2003 tax reconciliation bills among others. Mr. Zerbe holds an LLM in taxation from NYU and J.D. from George Mason University.

Mr. Zerbe, thank you for joining us today. We look forward to our conversation that is ahead.

And I now recognize the Ranking Member from New York, Ms. Velázquez, to briefly introduce our last witness appearing before us today.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Linda Miller served as the Deputy Director of the Pandemic Response Recovery Committee. She is one of our country's foremost experts on preventing and detecting fraud. Prior to launching her own consulting business, she was a Principal at Graham Thornton where she led the firm's fraud and financial crimes practice. She was also the Assistant Director in the forensic audits and investigative service group at the Government Accountability Office. She has a wealth of experience and has dedicated her career to helping organizations identify and manage fraud.

Welcome, Ms. Miller, and I look forward to your testimony. Thank you.

Chairman WILLIAMS. Thank you. And again, I appreciate all of you being here today.

Real quickly, just as a reminder, before recognizing the witnesses I would like to remind them that their oral testimony is restricted to 5 minutes in length. And if you see the light turn red in front

of you it means your 5 minutes has concluded and you should wrap up your testimony. If you go too long I will give it a little of this (gavel tapping). You will hear that. Okay?

I now recognize Mr. Breeden for your 5 minute opening remarks.

STATEMENTS OF RICHARD BREEDEN, CHAIRMAN, BREEDEN CAPITAL MANAGEMENT, LLC; JT TAYLOR, SENIOR DIRECTOR OF FRAUD INVESTIGATIONS AND OPERATIONS, ID.ME; DEAN ZERBE, NATIONAL MANAGEMENT DIRECTOR, ALLIANTGROUP; LINDA MILLER, CEO, AUDIENT GROUP, LLC

STATEMENT OF RICHARD C. BREEDEN

Mr. BREEDEN. Thank you very much, Chairman Williams, Ranking Member Velázquez, Members of the Committee. I am honored to be here and appreciate your invitation.

For about 35 years, perhaps a little more, about half my life, I have been involved in efforts to combat fraud, to help victims of fraud overcome the ravages of the crimes committed against them, and in many cases to try and recover money that has been stolen from the public.

I have done that in a variety of settings in both the public sector and the private sector. I worked in the White House under Presidents Reagan and George H. W. Bush, 41, and during the time working in the White House for 41 I was very actively involved. One of the principal draftsmen of the legislation known as FARIA that helped solve the savings and loan crisis, which has involved a great deal of fraud and the legislation contained quite a few provisions intended to help recover the monies that had been involved in fraudulent loans.

I was Chairman of the SEC for just under 4 years, and every single day involved fighting fraud. That is what the SEC does among other things but it is a never ending struggle and in any marketplace there are people who will abuse the market. And the SEC, for every day I was there, we were involved in antifraud efforts.

And for the last 20 years I have administered a series of funds for victims of fraudulent activity. The last few years I have served as head of the Madoff Victim Fund on behalf of the Justice Department, and my firm works for both the Department of Justice and the SEC in administering funds for victims. A big part of that work is making sure to help make sure that the money in these funds makes it to the intended victims is to make sure that we identify and block false claims.

So your topic today is very important. It is near and dear to my heart but it is important to taxpayers, to the SBA and its work and to faith in our institutions. So it could not be more important.

About 11.4 million loans were made in the pandemic programs. In our work over the last 35 years, I have never seen a program with fraud incidents lower than roughly 30 percent. If government puts up a billboard that says, "free money, apply here," lots of people will come. And unfortunately, not all of them are entitled to participate.

So I think the estimates, we will never know the total amount of fraud but the estimates even at the high end of 200 billion could be conservative. That is just the world we live in. And I think it

is important as was mentioned to remember the time pressure that we were under and the great, great good that these programs accomplished. And nothing in the later efforts should take away from that.

The amount of fraud, the SBA has estimated 25 billion; GAO, 200 billion. It could be 400 billion. We will never know. There was an ocean of fraud and now the question is how much of the improper funds can we get back?

There are a lot of ideas. My written testimony lays out a number of ideas as do the other witnesses. But I think overall the 100 years of fraud and 100 years' worth of investigations that I certainly have no problem. When I was at the SEC, we were always trying to make sure we had enough resources. And making sure that OIG has enough resources is an important question.

But we do not have 100 years. And if we give them more resources, and it takes 3 to 5 years to train somebody to know what they are looking for, our time, and even on an extended statute of limitations will run out. So the goal to me should not be let's figure out how to get 100 years to 93 years or 86 or 72l; it is how do we accomplish the most we can possibly accomplish over the next 5 years.

To do that I would say we have to supplement the resources that exist, whether at current levels or enhance levels, but find ways to break up the caseload, bring other people onto the playing field, and use the private sector to go after some of the bad actors.

I suggest in my testimony forming small groups, private sector contractors. Medicare and Medicaid do something similar. The SEC does it. The DOJ does it. Other agencies do it so I am not certainly having something totally innovative but in this area I think it could pay great dividends.

Most importantly is to have a mentality of an outrageous sense of urgency here to get after this problem and get as much done as possible. Thank you, sir.

Chairman WILLIAMS. Thank you.

And I now recognize Mr. Taylor for his opening remarks.

STATEMENT OF JT TAYLOR

Mr. TAYLOR. Thank you, Mr. Chairman.

Chairman Williams, Ranking Member Velázquez, and Members of the Small Business Committee, I am honored to be here today.

My name is JT Taylor, and I serve as the senior director of fraud at ID.me.

Before this role I dedicated a significant portion of my professional career to the U.S. intelligence community and the U.S. military, serving in both as an intelligence operations officer. Later, I served as a special agent with the United States Secret Service, where I led a series of pivotal domestic and international fraud and cybercrime investigations.

My tenure in intelligence operations and my investigative endeavors have granted me a comprehensive and nuanced perspective on the challenges inherent to digital fraud and cyberthreats.

When the pandemic gripped our world, governmental bodies like the Small Business Administration and the Department of Labor stood on the frontlines swiftly allocating relief funds. However,

haste led to vulnerabilities in security and identify verification. The SBA's Office of Inspector General identified worry signs. Numerous IP anomalies pointed towards foreign intrusions and coordinated fraud attempts. The misuse of employer identification number was rampant with multiple PPP loans under single EINs.

Furthermore, there was a starting discovery of businesses declaring post-deadline establishment dates and recurring use of identical contact details across different applications.

The funding system supporting these initiatives are intrinsically linked with the broader business ecosystem. Conventional practices involve businesses contributing to benefit funds calibrated on their workforce size.

But the massive, unexpected unemployment claims threaten this balance. State debts have increased and there is now an impending risk of businesses, particularly smaller ones, facing escalating per employee taxes. This is a multi-dimensional problem with repercussions for the entire U.S. economy.

The pandemic served as a double-edge sword. On one side is unveiled resilience and adaptability of our institutions. On the other it exposed areas where we were woefully unprepared, chiefly in the arena of cybersecurity and fraud detection.

In these challenging times, states sought robust, scalable solutions. Twenty-seven states turned to ID.me which is not just another tech company but a leading credential service provider. Independently certified against rigorous standards set by the National Institute of Standards of Technology, ID.me embodies the pinnacle of digital identify verification.

Supporting a user base exceeding 113 million, the impact of ID.me on fraud prevention has been profound. Partner states witnessed transformative results. Fraud rates drastically diminished. Authentic claims experienced seamless processing and financial savings were substantial.

Beyond the monetary gains, the rejuvenation of public trust in an era when faith in public institutions is fragile is invaluable. In this digital era, standards like this curated by NIST are not optional but foundational. Overlooking these guidelines as seen sporadically during the pandemic leads to compromising security.

In today's digital world, data has emerged as a prime commodity. Amid this landscape, data brokers who amass, refine, and frequently monetize user information have risen in prominence. Although they often work within current legal constraints, their vast data repositories offer a Goldeneye for malicious entities.

The financial drain due to digital fraud during the pandemic serves as a testament to the perils posed by easily accessible data. There is an urgent need for our defense mechanisms to adapt considering this threat landscape. A comprehensive strategy that merges the strengths of both the private and public sectors is imperative.

The Macomb School of Business from the University of Texas at Austin revealed that a concerning 11 percent of PPP loans exhibited suspicious traits. Notably, the top 12 lenders with the highest rates of suspicious loans are all Fintech lenders. Given the disparity between the statute of limitations for bank fraud and wire

fraud, it is imperative that Congress takes action to address the inconsistency, particularly in the context of the PPP loans.

In addressing the multifaceted nature of fraud, a dual pronged approach is essential. First, we bolstered the collaboration of data sharing across agencies. By harnessing the capabilities of the Pandemic Analytic Center of Excellence and fostering deeper ties within the private sector, we can integrate data matching earlier in the benefit payment cycle.

Simultaneously, it is crucial to democratize data validation tools. The Social Security Administration's electronic consent based Social Security Number verification tool, currently exclusive to financial institutions, should be extended to approve credential service providers. Such an expansion would ensure equitable access benefitting a broader demographic and further strengthening our antifraud measures.

Agencies should adopt digital identity solutions such as those perfected at ID.me with strict adherence to the NIST 800-63-3 guidelines. This ensures robust identity proofing minimizing fraudulent access and upholding the integrity of public portals.

In our collective journey—and the challenges of the pandemic, it is imperative that we absorb its lessons. Our trials and triumphs underscore the essence of teamwork, innovation, and unwavering commitment to establish identity verification protocols. Whether it is the commendable work by organizations like ID.me or the diligent oversight by entities like SBA OIG, we have seen the potency of dedicated efforts. We are urged to build on this momentum, reinforce our defenses, honing our strategies and equipping ourselves better. The American people deserve benefit programs that prevent, detect, and recoup fraudulent payments.

I thank the Committee for this platform, and I am happy to answer any questions you may have.

Chairman WILLIAMS. Thank you very much.

And let me just say this. You are going to see people coming and going. They are not leaving. We have got other hearings. They will come, they will leave, and so forth, so if that is something you were wondering about that will happen.

Next, I want to recognize Mr. Zerbe for his 5 minute opening remarks.

STATEMENT OF DEAN ZERBE

Mr. ZERBE. Thank you, Mr. Chairman. Thank you, Ranking Member, for having me today at this important hearing about how to recover funds that were put forward in the SBA COVID Relief Program.

I am coming forward today to talk about a specific bipartisan solution that has had bipartisan results over the years recovering billions of dollars in other government agency programs, namely basically rewarding and incentivizing whistleblowers to come forward and lay out the details of fraud that they are seeing.

Just as a quick background on me, Mr. Chairman. You laid it but specific to this you said I worked for Chairman Grassley on the Senate Finance Committee. I wrote the IRS whistleblower law that then served as the model for the SEC whistleblower law and the

CFTC and other government programs. And I now also practice as an attorney in this area representing whistleblowers.

I would just say that the benefits of a whistleblower program are pretty straightforward. First of all, you have to understand in fraud, fraud is purposely being hidden. It is hidden in the nature of it. If you want to get it, you have got to get insiders with informed, knowledgeable detailed information. That is how you uncover fraud, and study after study has shown that. And we have seen that, for instance, in the IRS programs. They did not know beans about what was going on with offshore accounts until a whistleblower came in and blew it all out for them. The whistleblowers give you the keys to the kingdom in terms of what is going on. So they are a proven way to do it.

I think in particular that it is useful for the SBA to consider this because of the resource limitations and where they are going. The idea of the whistleblower is that they are going to help the government agency, whichever it is, better target and package and go after the bad actors. In other words, when I am filing a whistleblower complaint, I can assure you it is with a bow on it and on a T-ball in terms of what I am trying to do because I want to provide a narrative of what is going on. I want to provide all the documents. I want to provide everything from teeth to tail of what is happening. Why? Because I want to get the agency to move so that my client can get paid. So you are doing a lot of the lift for the agency in terms of assisting them in terms of the work. You are also doing a better job for the agency of helping them target the bad actors. Even the best government agency has a difficult time identifying, okay, who is really here? You have the whistleblower coming in. They know who the bad actor is. They have got the goods on them and they are much better at identifying, which actually is the positive of leaving the honest folks out there alone. So you are better targeting resources as well, too, with that. So I think with the SBA that is good.

I think another thing that is helpful here is in reading the SBA IG's reports, they clearly have a culture of embracing whistleblowers and that is terrific. Clearly, they are bringing folks in. They are taking that. One of their biggest cases that they mentioned in the white paper was hundreds of millions of dollars from one whistleblower. And what you are trying to do is build that out and encourage more whistleblowers to come forth, particularly well placed, knowledgeable, informed insider whistleblowers that are coming forward. So I think you are benefitting from the fact that the SBA already has got a welcome mat forward and you are trying to expand beyond that in terms of it.

One thing I think will be music to ears—since the time from being a staffer on the Senate side is CBO should score this. They should score this as a revenue raiser. They have scored other money. I am sorry, other whistleblower programs. The AML bill that just passed scored $4 million. I think all these scores are low by the way. For instance, my program, they scored it out at I think a few hundred million dollars joint tax. It has brought in billions of dollars since it came in. But they will score it and your staff will work with them and I am sure get that there.

The other thing I want to mention is the deterrent ability of whistleblowers. Look, when you are out there as a fraudster and all you are thinking is, well, I have just got to get it by those folks over at the agency, that is one calculation. If you have got a whistleblower program they have got to say, okay, well, now I have got to trust everybody else in this room. I have got to trust my banker, my secretary. Any of them can dime me out. And so it changes dramatically the way the equations go of can I get away with it? It also affects their behavior. What we find in tax is that they are constricting who is involved. They try to limit what it is so it has an impact on their behavior. It has a deterrent impact as well, too.

The last thing I would just note just on a highlight, my written goes into it more, I think four hallmarks for a good whistleblower program, one having a mandatory award program, not discretionary. Have a floor and a ceiling based on the amount recovered broadly defined. You want a dedicated payment so that the funds are there. You are not having to go run to the approp boys to get dollars for it. And these are standard by the way. What I am laying out is what we have in all the whistleblower award programs. Have an established office within OIG that wakes up thinking about the whistleblowers and is putting out the welcome mat for them. And then you have independent review.

The whistleblower, look, when you are getting very good whistleblowers I am getting not just, you know, Billy in the dark room. I am getting the vice president of Tax coming forward. They are putting their life at risk in terms of doing this. They need to have confidence. It does not mean they are going to be guaranteed a payment but if their provided information is used and it ends up collecting money, they are going to get a fair shake and that somebody independently is going to look at that. It is not just to the whim.

So I thank you, Mr. Chairman, having me here today. I appreciate it very much.

Chairman WILLIAMS. Thank you very much.

And now we recognize Ms. Miller for her 5 minute opening remarks.

STATEMENT OF LINDA MILLER

Ms. MILLER. Thank you, Chairman Williams, and Ranking Member, Ms. Velázquez, and Members of the Committee.

I sit here today as a former Olympic athlete, a former government executive, a former partner at a large accounting firm, and a small business owner. And I am bringing all of those perspectives to my comments today.

I spent my career working to help the government fight fraud. I led the development of the GAO framework for managing fraud risks in federal programs, and worked with Congress to draft the Fraud Reduction and Data Analytics Act of 2016.

When I was the partner at Grant Thornton, my team led the development of the Treasury Antifraud Playbook. I sat on the task force that developed the COSO Fraud Risk Management Guide which governs the private sector. I serve on the Advisory Panel of U.K. Public Sector Fraud Authority. And I sit as a Member of the Identity Theft Resource Centers Biometric Working Group.

As soon as PPP and COVID EIDL programs were unveiled, those of us in the fraud world saw this as a field day for fraud actors. We did not have to think about it to see how much fraud was going to happen in these programs.

An example, the COVID EIDL grant program was essentially money that was known to not need to be repaid back. Anybody that applied for that money got it without having to provide any eligibility information. And you know, at that point the only thing keeping somebody from stealing that money was their own moral compass. And that is not exactly a good fraud control.

At that time, the fear and desperation of America's small business was such that the decision to get this money out with few, if any controls to verify the eligibility of the information provided by borrowers was widely accepted. Speed was the goal.

From celebrities stealing PPP loans and buying luxury cars to adversarial nation state actors executing coordinated and elaborate schemes, there were staggering levels of fraud in these programs.

The finger of blame can be pointed in several different directions and it has been over the last 3 years. SBA had not seriously considered fraud risks prior to the pandemic and it was unprepared for the breadth and the sophistication of the adversary.

Congress created program rules and time pressure that made it nearly impossible for the SBA to verify the eligibility of applicants. And unscrupulous lenders looked for ways to game the system and pocket outrageous profits and fees.

Today, the work of clawing back the stolen pandemic loan funds is left to the SBA OIG and its law enforcement partners. As the deputy executive director of the PRAC, I worked closely with Mike Ware, SBA's Inspector General. IG Ware and his team have worked tirelessly to investigate and prepare for prosecution thousands of fraud cases and the work has only begun.

Thanks to this Committee, Congress has recently extended the statute of limitations on pandemic fraud to 10 years. And given the caseload, the IG is going to need at least that long to bring fraud actors to justice.

For the past 3 years, the SBA Inspector General's work has yielded a 200 percent return on investment. But its backlog is enormous and the office is stretched thin. This is not the time to cut the Inspector General's budget. Funding the IG at his requested levels will ensure this exceptionally productive work can continue.

But the backlog is not just with investigators. Bringing fraud actors to justice requires prosecutors to try those cases. The U.S. attorneys are also stretched thin, and there is no shortage of high quality cases to prosecute. Innovation in recouping pandemic loan fraud must require more than simply putting good cases on the U.S. attorneys' desks.

Today's hearing is also exploring the role of identity theft in pandemic loan programs, so it is important to note that identity theft plays a role in loan fraud, but it was not the largest driver of fraud in PPP or COVID EIDL. Front end identity verification technology, including remote biometrics, is but one tool in SBA's toolset and it is by no means a panacea.

Fraud actors created shell companies, often using stolen information to apply for loans. But this type of identity theft base fraud

is uncovered through conducting due diligence on the information in those applications and SBA has done quite a bit more of this due diligence to date. They now require tax transcripts of loan applicants. They use vendor information to verify a bank account. And they flag certain EIN prefixes, none of which was done at the start of the pandemic.

Despite these improvements, SBA does have more work to do. They have to continue to mature their preventative antifraud capabilities. They must adopt a culture that is conducive to fraud risk management and they have to collaborate with the OIG to ensure that lessons learned are incorporated into their antifraud controls.

I was a rower in the 2000 Olympics, and as such I know a thing about teamwork. My career has straddled the public and private sectors for a reason. Because I believe that the government and the private sector make a powerful team. The government relies on the private sector innovation, and the private sector requires services like main street saving loan programs that only the government can provide.

I look forward to discussing the productive ways the private sector can assist the government in recovering loans and preventing fraud going forward. Thank you.

Chairman WILLIAMS. Thank you very much. And good job on the 5-minute rule. It is great.

I will now recognize myself for 5 minutes.

When I first heard about the 200 billion dollars in potential fraud in the SBA pandemic lending programs, it made me think about how a business owner would act in this situation. They would have to decide whether they do all they can to collect the $200 billion that is on their books as a receivable, or to write it off as a loss. No private entity has the luxury of writing off such a massive number, so I think it is our duty to be good stewards of the taxpayers and find ways to give this money back which we have already begun to talk about.

The SBA's Inspector General told us that they currently have over 100 years of casework if they are going to investigate all the loans that have been flagged for fraud. This is obviously an impossible task and there must be a better way to help them get this money back.

So Mr. Zebre, during your time as senior counsel to the Senate Finance Committee, you crafted legislation under Senator Grassley to overhaul the IRS whistleblower program as you said and my team and I are exploring the idea of creating a similar, self-sustaining program which will allow any citizen to collect a commission if they report COVID fraud that results in money returned to the Treasury.

So the question is, do you think it would be possible to create this type of program that would empower every day Americans to report fraud? And what are some of the things we should be aware of as we look to create this program?

Mr. ZERBE. I think that is an excellent question, Mr. Chairman.

I have seen it. A number of government agencies have created these whistleblower award programs. And so I think very much SBA is a good possibility in terms of also looking at creating a whistleblower award program. You already have the Qui Tam

False Claims Act where they are bringing a few cases in right now from attorneys from whistleblowers and that has had some success. But I think having in parallel with that an in-house whistleblower award program will very much be a way to, as you say, commission to bring in the energy of the whistleblowers that are attorneys, that are advisors, to help the SBA move forward. So yes, I think it is a very good candidate for the SBA to look at doing. Absolutely.

Chairman WILLIAMS. Great. Thank you.

Mr. Breeden, you are currently working as special master for the victims of Bernie Madoff's Ponzi scheme. This requires you and your team to go through massive data sets to find out what claims are legitimate and which ones are fraudulent.

So the question is, can you speak on how massive financial recovery is possible when there is such a large quantity of data to go through?

Mr. BREEDEN. Yes, sir. It is definitely a challenge. In the Madoff Victim Trust which I administer we have had about 70,000 claims covering $80 billion in claimed losses. We have approved about 10 billion of that. So there is always a significant difference. And some of it is legitimate, and some not between what gets originally claimed and what you end up approving after you have reviewed it very carefully.

We have had data documents, brokerage statements and so on from victims going back 20 years. Millions of pages of documents covering hundreds of thousands of transactions. And I love technological systems. Our company, our victim trust, we use systems to scan things all the time. But the most effective tool is an experienced person sitting looking at the analytics and deciding that there is a problem that needs greater follow up. So big data can do a lot of things but it is not going to haul crooks in to identify and have someone go after them. So it is a mix of systems and trained people.

And one of the problems we have today is starting now to bulk up investigative resources in the SBA, for example, that is great but it takes 3 to 5 years to mint somebody that really knows what they are looking at. And so you have got to lag ineffectiveness. I think it is still possible. We have done the Madoff work and identified thousands and thousands of improper loans, and some that were referred for prosecution and that have generated recoveries but that is not our principal role, with a relatively small group of people. And that is why I think the combination of mini-SWAT teams that are focused on recovering money and focused on reading the, you know, out of 12 million loan files. All right. Suppose you took the 100,000 largest loans and have people who know what they are looking at read the files and look at where are the cases that are best cases to prosecute?

Chairman WILLIAMS. Thank you. My time is up and I now recognize the Ranking Member for 5 minutes of questions.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Ms. Miller, we have established that the Inspector General and law enforcement are the lead organizations to investigate and recover fraudulent monies. What is the most important action that we can take to help recover stolen funds?

Ms. MILLER. Well, if we want to recover stolen funds, the action needs to be focused at the IG because the IG and the law enforcement partners of the IG are the only entities who have the authority to do investigations and prepare cases for prosecution.

Ms. VELAZQUEZ. In your opening statement, you mentioned the fact that we passed the law to extend to 10 years to go after the bad actors. Through the legislation we gave them, OIG, more time but now they need the resources. If the OIG is not fully funded we will not be able to capitalize on these two new laws; correct?

Ms. MILLER. Correct.

Ms. VELAZQUEZ. Mr. Zerbe, IG Ware testified before our Committee that their HUD line produced 90,000 actionable leads that will take more than 100 years to examine. The law enforcement community has said they need more resources to investigate, prosecute, and recover fraudulent monies.

How does your proposal meet the needs of the law enforcement community and improve prosecutorial outcomes?

Mr. ZERBE. Thank you for that.

Just one quick note. When you are talking about Mr. Madoff, I cannot help but note that it was a whistleblower, Mr. Markopolos, that revealed Mr. Madoff. Just as an aside.

I think that is an excellent question. I think it is twofold. When you are incentivizing whistleblowers, it is one thing to get a tip that they may get at SBA that is of some use but these tips kind of tend to be, hey, I saw a guy at a bar and he had a fancy car. I mean, they are not that useful a lot of them. And when you are incentivizing a whistleblower and encouraging, they are going to come in with a full package. They are going to come with a lot more detail, much more robust assistance in terms of what is going on. So really helping the agency do its work. So helping them expand their work.

But to your point, too, and one thing to consider, maybe this is a way to split the baby is that a number of the whistleblower award programs do allow for a partial recovery of the funds for the IG shop itself. In other words, HHS IG with the Qui Tam program. They basically get reimbursement for their investigations. CFTC similarly with their whistleblower program, they get to reimburse their costs for their expenses for these whistleblower programs. So it kind of aligns everyone's behavior. So something maybe for the Committee to think about of a way to finesse the issue. But that would be now it is. Primarily, it is allowing the agency to work more expeditiously, ma'am.

Ms. VELAZQUEZ. Thank you.

Ms. Miller, in your view, would this proposal be a more cost-effective way to recover fraudulent funds as opposed to fully funding the Office of Inspector General and the law enforcement community?

Ms. MILLER. I mean, I would not say that we should do that instead of fully funding the Office of Inspector General. I could not speak to how much that is going to improve prosecutorial outcomes but it is possible. It will cost money. You will have to create an office, and you will have to pay those people salaries. And so the scoring could come back.

Ms. VELÁZQUEZ. Here we are at the brink of a government shutdown over the budget; right?

Ms. MILLER. Right. Exactly.

Ms. VELÁZQUEZ. Okay. Mr. Taylor, privacy advocates have concerns about the large amount of data ID.me collects to verify users' identities—data like Social Security numbers, military records, bank and credit card records, biometric data, and government documents. Does your company share this data with third parties?

Mr. TAYLOR. Thank you for the question, Ranking Member Velázquez. I appreciate it.

Our privacy policy is one of the most robust in the industry. I would counter that our privacy policy is actually even more stronger than the average grocery store that you visit on a daily basis. We do not do any type of selling or trading of personal data. Additionally, from a standpoint——

Ms. VELÁZQUEZ. To be clear, you do not sell or share this data with third parties?

Mr. TAYLOR. That is correct, ma'am.

Ms. VELÁZQUEZ. Okay.

Mr. TAYLOR. No selling or trading——

Ms. VELÁZQUEZ. Does ID.me benefit monetarily from the data provided by American citizens?

Mr. TAYLOR. ID.me makes money via the actual identity verification itself and successful transactions, meaning successful identity verifications versus transaction based.

Ms. VELÁZQUEZ. Thank you.

Mr. Breeden, based on your experience overseeing the Madoff Victim Fund, could you please share any lessons learned from your experience that could help law enforcement recover from pandemic fraud?

Mr. BREEDEN. Well, thank you.

In addition to Madoff I did WorldCom and Enron and British Petroleum and a couple of JPMorgan cases. And so I have actually reviewed, my staff and I, about 150 people all told over 20 years. Have reviewed over 4 million claims to these victim funds.

Chairman WILLIAMS. Time is up.

Ms. VELÁZQUEZ. Thank you.

Chairman WILLIAMS. Time is up and we can put that in writing if need be. Okay.

I now recognize Representative Alford from Missouri for 5 minutes.

Mr. ALFORD. Thank you, Mr. Chairman and Ranking Member, for holding this important, very important hearing today. And thank you for our witnesses, all of you, for being here.

We are here for one reason and one reason only. In the words of Jerry Maguire, "Show me the money." This is taxpayer money we are talking about here. Congress knew that this money had to get out the door fast. We had an economic crisis from the pandemic. So the House and the Senate came together to do just that. Some fraud was expected but not $400 billion worth of fraud on the American taxpayers.

I am still disgusted that Administrator Guzman would not bother to come down here and talk to us about her lower projects of fraud

and what she is doing about it to get that money back for the American people.

That is why we introduced 3 weeks ago the CAB Act. We cannot get inside the Small Business Administration to go visit Ms. Guzman. We want to change that. The Congressional Access to Bureaucratic Officers. According to the Inspector General's report, 33 percent of all EIDL loans were estimated to be fraudulent. These loans were administrated solely through the Small Business Administration. And I know that Administrator Guzman released a report contradicting that but let's stick to the fraud, abuse, and misuse expert, the IG.

This is in stark contrast to the PPP loans which are only 8 percent estimated to be fraudulent. These were loans administrated through lending partners, private businesses who could get it done right.

The first step in solving any problem is recognizing that there is one and addressing the issues. Clearly, there are problems. We are here today to find answers.

Mr. Breeden, I want to start with you. You talked about in your testimony a couple of quotes. Remember the good in this program at the time that we had it, up to $400 billion as we are now recognizing. You call it an ocean of fraud which I think is very apt. Does the good outweigh the bad in this program?

Mr. BREEDEN. I do not know that I am qualified to answer that. I think we were faced with a crisis the likes of which in my lifetime I have never seen. It would have been nice to be tighter in how we handled it. We did not. That is water over the dam from my perspective. The question is how do we go after the money that was taken improperly?

I have spent 20 years doing that for the SEC, for the Justice Department, and you do not do it by writing reports. You do it by taking the largest transactions, going through them, putting knowledgeable people reviewing it, and where you find problems, refer it, get teams and prosecutors to go after it. And we have to remember that iceberg of stolen money a few years from now will be an ice cube. Time is of the essence.

Mr. ALFORD. Well, clearly we do not have the resources to do this right now with the Inspector General's office. You are proposing the private sector fill in the gaps. Could this work with the whistleblower program? Put everyone on commission and lets get this $400 billion back.

Mr. BREEDEN. Yes, sir. I think you could. That is what I am suggesting that other agencies supplement their internal sources with people on the outside. I have for the last 10 years worked for the Department of Justice. I am not a government employee but under contract we work for them. Every day we try and find fraud and refer it to prosecutors.

Mr. ALFORD. Are there any prosecutorial risks once we get to court with these when the private sector is involved versus someone with the government?

Mr. BREEDEN. None whatsoever.

Mr. ALFORD. There you go.

What do we learn from this now? Really quickly, can you give me one thing that we can improve on next time, God forbid we have another emergency like this?

Mr. BREEDEN. A little slower. A better pace. Systems knowing ahead of time you are going to have a lot of fraud and that you have to go through the data as you make each and every loan. It is way better for the taxpayers to stop the fraud before it happens then to go after it later.

Mr. ALFORD. Thank you, sir.

Ms. Miller, quick question. You said you worked with the Inspector General on this. Have you met with the Inspector General?

Ms. MILLER. Yes. Many times.

Mr. ALFORD. Have you met with Administrator Guzman on this topic?

Ms. MILLER. No.

Mr. ALFORD. Why not?

Ms. MILLER. I worked for the Pandemic Response Accountability Commitmtee, so Mike Ware, the IG is a Member of that Committee. So I worked closely with him. I did not have a reason to meet with——

Mr. ALFORD. If you happen to talk to her would you tell her we would really like for her to come down here and explain the differences between her number and the number of the IG and what we are going to do to get this back? Would you do that for me? Thank you very much.

Ms. MILLER. Yeah, I have some ideas about the differences, too, I could share.

Mr. ALFORD. Well, thank you very much. I yield back.

Chairman WILLIAMS. Thank you. I now recognize Representative Davids from the great state of Kansas for 5 minutes.

Ms. DAVIDS. Thank you, Chairman. And thank you to you and to the Ranking Member for holding this hearing today.

As several of our witnesses have already pointed out, combatting waste, fraud, and abuse of government dollars should be something that we are all interested in. The Small Business Administration's COVID-19 relief programs, like the Paycheck Protection Program and the Economic Injury Disaster Loans certain saved countless small businesses from closing. But unfortunately, American taxpayers and many other small businesses were victimized by fraudulent actors that stole those desperately needed funds, a total of which is estimated to be over $200 billion. And to date the SBA and Office of Inspector General have successfully recovered about $30 billion in fraudulent COVID-19 funds.

But certainly, there is more work to be done. Given the unprecedent scope of these pandemic programs, we have a lot ahead of us. But I know we are currently responding to pandemic-related fraud. But we also need to be prepared to properly mitigate widespread fraud during future emergencies. And that means ensuring that our government oversight resources are prepared in utilizing the best practices that we have learned during the COVID-19 pandemic. I do think that everyone here today shares a common goal of protecting American taxpayer dollars and ensuring that we are being fiscally responsible while doing that.

So before I dive into my question I do want to thank all of our witnesses for sharing your perspectives, for your service, and making sure that we have a better stewards of the taxpayers' dollars.

So the first question, Ms. Miller, I would like to ask you. Given the SBA OIG has shared this concept of 100 years' worth of pandemic-related casework to properly review, review the cases, I am curious how you—maybe you can share some of the insights you have about how we can better prevent the fraud, waste, and abuse going forward as we look at—not if, but when we face future emergencies.

Ms. MILLER. Yes. And I think that is a really important point because we are talking about recovering pandemic stolen funds today, but it is water over the dam. And it is really important to prepare agencies for the future. SBA had not implemented many, if any, of the practices of the GAO framework for managing fraud risk in federal programs which GAO issued in 2015. The comptroller general has made comments publicly in several hearings about his disappointment that agencies did not take that document more seriously and follow those practices.

And so going forward, SBA has begun to take some steps. They have established a Fraud Risk Management Board, which is a good, centralized entity that shows some commitment. But they need to continue to build, and all agencies, especially SBA and anybody that is administering a lot of direct funding to the public, preventative antifraud controls that use data. And that is really important. SBA has begun that work but there is much more work for SBA to do in the future if they want to make sure that they can be prepared for the next.

And I want to make a point about recovering funds. A lot of the funds that were stolen were identity theft funds. Those were nation state actors. We are not going to get those back from whistleblowers or anybody else. They are gone. We are not going to get that money back, unfortunately.

Ms. DAVIDS. So one of the things that I did want to ask you about as well as the suggestion of incentivizing whistleblowers. I am curious in your view with the SBA OIG in their current capacity housing some sort of whistleblower management office what, really quickly, if you could tell me what your thoughts are on that.

Ms. MILLER. Yeah. I mean, they are going to have to add staff to fund that office. And so, you know, given that the IG is already stretched, you know, it could be. I am really not qualified to weigh in on the cost benefit of it but it would definitely add resources, and the SBA OIG has mentioned that he needs more resources than he already has now. So that has to be considered.

Ms. DAVIDS. I am low on time.

Mr. ZERBE. If I could add to the conversation.

Ms. DAVIDS. Oh, yeah.

Mr. ZERBE. The only thing I would just say to that is I do not know the details either but I would say it may be minimal because they are already dealing with folks coming in with tips and resources in the thousands. So I do not know if it is going to need a big expansion. I am sorry.

Ms. DAVIDS. No, I appreciate that.

In the limited time I have left, I might follow up with all of you with some of the additional questions I have but I do want to highlight a couple of things, particular from the voices from the private sector. One of the things that I have noticed is that some of our systems of data management and vetting probably need to be updated and upgraded. And that might also be something that the private sector could be helpful with SBA on. From this Committee's perspective I might follow up questions on that as well. Thank you.

Chairman WILLIAMS. I now recognize Representative Bean from the great state of Florida for 5 minutes.

Mr. BEAN. A very good morning to you, Mr. Chairman. And good morning, Small Business Committee. I have been cheering over the weekend so my voice is here but I got just enough to get through 5 minutes of questions. Panelists, it is very good to see you this morning.

Here is the biggest thing. We do not agree on much but we do agree that there is fraud. We all agree that there is fraud. Here is the numbers. Here is the discrepancy of disagreement. Secretary Guzman says there is only 36 billion in fraud; yet, Inspector Ware says maybe there is 200 to 600 billion. Which is it?

Ms. Miller, do you want to start us off?

Ms. MILLER. Yeah, well, I think that it really depends on how you define it. So the SBA believes that certain EIDL loans and certain PPP loans should not be considered fraudulent because, for example, if an EIDL loan is in repayment the SBA believes that a loan that is in repayment, it is illogical to consider that that loan would be fraudulent. The SBA IG does not agree. So they do not agree on the terms.

Mr. BEAN. Gotcha. But that number is bigger than 36 billion you think?

Ms. MILLER. We do not know. I mean, I do think it is bigger than 36 billion.

Mr. BEAN. Let me go to Mr. Breeden. You say that number is bigger than 36 billion?

Mr. BREEDEN. Massively bigger.

Mr. BEAN. It is. I think that is the correct answer that it is bigger than 36 billion.

Mr. BREEDEN. In 35 years I have never seen a program with less than 30 percent roughly false claims. So that puts you at a much, much higher number.

Mr. BEAN. They come out. One of the hardest things that I have had to deal with, I guess, and maybe you are familiar with it. And it deals with Barbie. I do not know if you are familiar with Barbie. You know about Malibu Barbie or Presidential Barbie, but we now have Swindler Barbie. And I want to show you some of the actual logins that our vendors accepted as real people. And you can see behind me right now.

Mr. Taylor, are you familiar with this? Are you familiar with the scam that was run?

Mr. TAYLOR. I am, sir. What you are looking at is a mess that made it through Fintech platforms.

Mr. BEAN. I gotcha. Now, what can we do in the future so that Barbie or Ken—he got in on this action, too, by the way—what can we do to prevent Barbie and Ken from getting in on the fraud?

Mr. TAYLOR. At ID.me, we deal with Ness 1:00:43xx quite regularly. We stop them in their tracks through something called Presentation Attack Detection, sir. PAD.

Mr. BEAN. So there is software that we just did not employ or did not use?

Mr. TAYLOR. That is correct, sir. Whenever we get somebody on camera we ensure that they are a live person.

Mr. BEAN. Very good. Would it shock any of you, I just read an article this morning that Tencent, a big Chinese company that is a major investor in Womply, which is one of our vendors, we paid them $2 billion to administer this fraud. Would that shock anybody that we paid Beijing to make sure that this fraud happens?

Mr. Breeden, does that shock you?

Mr. BREEDEN. No, sir.

Mr. BEAN. Yeah. We call this Crazy Town for a reason a little bit.

Here is just a toss up question I have. The frustrating thing is there was talk of just letting smaller loan frauds go. Just saying, you know what? We will just let that go. But I say no. I say no, and I think everybody up here says no. I filed the "We Want Our Money Back Act," which says we want our money back and we are not going to let it go. And so I have that bill. There are other bills that say lets extend the statute of limitations to go after it. There is another bill that says anybody that is suspected of fraud shall be prohibited from any government program until it is worked out. I think that is a great bill, too.

What else do we need to do? What else do we need to do to get our money back?

Ms. Miller, jump in.

Ms. MILLER. Yeah, well, one thought is that you can offer amnesty to those people who pay back the money. Amnesty from prosecution for those individuals that are willing to voluntarily give the money back. I suspect there are a number of people who have the money and they know that they got it erroneously. They got it fraudulently. And if they thought they were protected from prosecution they might give it back.

Mr. ZERBE. Can I—I am sorry. Go ahead.

Mr. BEAN. No, go ahead. Go.

Mr. ZERBE. I would add that the IRS is facing the same level of fraud in the Employee Retention Credit Program. And the amnesty is something that they are basically putting out there to say why don't you come in and meet Jesus and get right. So that may be something to consider as well.

Mr. BEAN. Ten-four. Thoughts, Mr. Breeden?

Mr. BREEDEN. Wanted dead or alive posters probably have a long history in reward programs, whether you call them whistleblowers or something else are certainly part of the solution. But I go back to if you have got a problem that you think you might have had 3 or 4 million bad loans, you cannot wait 100 years. So put together teams of people, parcel those out, and start looking.

Mr. BEAN. Thank you very much.

Mr. Chairman, I have run out of voice and I have run out of time. I yield back.

Chairman WILLIAMS. Thank you very much.

I now recognize Representative Scholten from the great state of Michigan for 5 minutes.

Ms. SCHOLTEN. Thank you so much, Mr. Chair. And thank you to the witnesses for coming here to testify today about this truly important topic.

I want to start by saying that the 1.2 trillion in aid that the SBA has distributed over the course of the pandemic was truly essential, a lifeline to so many businesses in keeping their doors open. And in the context of this important discussion today I do not want to lose sight of that. You know, I think that there is a lot of agreement here today about the frustration over the inability to pinpoint how much fraud there was because a lot of our constituents, many of our constituents were struggling to make ends meet during the pandemic, and their hard-earned tax dollars were going to fund these programs.

Ms. Miller, in your testimony you state that the truth most likely lies somewhere in the middle. I am a future-oriented, problem-solving individual. You recommend that Congress establish a well-funded—more taxpayer dollars—centralized antifraud office. Can you elaborate on how this would allow the federal government to prepare for the next emergency and how we might be able to avoid this type of situation in the future?

Ms. MILLER. Sure. Yeah, cross governmental, intergovernmental agency issues are notoriously difficult to solve because every individual agency is focused on its mission and its budget. And so getting them to coordinate their activities is always very difficult. We knew this when I was at GAO. We talked about this a lot.

This is an intergovernmental problem. It crosses all of government, both federal, state, and local. You need a centralized entity within the federal government that is not the Inspector General. The IG's job is to get the money back after it has been fraudulently obtained. The agencies, like the SBA, are the ones that are responsible for preventing the fraud to begin with. But each individual agency, if working together, can do things like sharing data.

Like, for example, it may not be known that the "Do not pay," the Treasury "Do not pay" portal currently today does not have access to the Social Security Death Master File as we speak, 3-1/2 years after the pandemic. I mean, that is a problem of data sharing and collaboration and creating data use agreements. The Pandemic Analytic Center of Excellence has created over 95 data use agreements between agencies. That is a model for what the government should do but not in the IG community; in the management side of the House.

Ms. SCHOLTEN. And as these recovered funds are coming back in to the Treasury, how does the government track these funds? Are there any transparency measures in place so that the public can watch and know the efficacy of recovering these funds and where they go?

Ms. MILLER. Yeah. The Treasury has an Office of Recovery Program and they also have an Office of Payment Integrity. And both of those offices coordinate the systems that provide that information to the public. So really it is the Department of Treasury that tracks that information.

Ms. SCHOLTEN. And how is that released to the public? Can we find that online? On the Treasury's Twitter account?

Ms. MILLER. Yeah.

Ms. SCHOLTEN. Is it a report?

Ms. MILLER. I think the Department of Treasury is actually really working right now in its Office of Payment Integrity to improve that transparency in the public-facing websites. And those are happening as we speak. I think that in the next year to 2 years we are going to see a lot of improvement in the information that is shared to the public. The PRAC also has a pretty great website that provides a lot of that transparency.

Ms. SCHOLTEN. Okay. I know I speak for many constituents that proactive communication about this and connecting that information to the public so that they can have confidence in this would be, you know, would be key.

Ms. MILLER. Agreed.

Ms. SCHOLTEN. Additionally, you know, in my last minute, I wonder if you might be able to pinpoint any steps that we might be able to take not only in preventing fraud or cracking down on it once it occurred but even putting steps in place to close the gaps to keep it from happening in the first place, are there more point to point contacts that we can ensure that the money is getting directly where it needs to go? You know, disseminating to local governments or nonprofit organizations first. Any and all of the above. Or if you have any insights as well.

Ms. MILLER. Yeah. I think that maintaining integrity of the funding that is going to citizens, whether that is through federally funded state administered programs, like SNAP or, you know, some of these benefit programs that go through the states or directly to the citizens from a federal agency. The importance is to identify quickly before the payment is made, and we have talked about this a bit today, whether or not the individual who is applying for that benefit is who they say they are and they are entitled to it. And that is going to require data. Data sharing. Data analytics. Advanced analytics that can use artificial intelligence and other tools and it is very vital that agencies get those tools to be able to prevent fraud, waste, abuse in the future.

Ms. SCHOLTEN. Thank you. I yield back.

Chairman WILLIAMS. The gentlelady yields back.

I now recognize Representative Meuser from the great state of Pennsylvania for 5 minutes.

Mr. MEUSER. Thank you very much, Mr. Chairman. Certainly, thank you to all of our witnesses here today.

A very important subject. Very troubling subject. I do not think the American people or taxpayers really have an understanding of the level of fraud that has just come out of a relatively small agency like the SBA. It certainly makes you think what levels of fraud occur elsewhere. You know, CMS. You name it.

So we have a big problem with this $5 trillion company of ours known as the United States federal government and the $6 trillion of spending that takes place. So your ideas, your backgrounds, experiences are very helpful to us.

So we had the EIDL, the PPP, and the ERTC. EIDL had a wildly unacceptable level of fraud, almost insane what occurred there. So

the investigations need to take place. PPP was a lot less, particularly on a percentage basis. PPP needed to be rushed. EIDL needed to be rushed. So it is not necessarily about assigning blame or which administration but a lot of times you have got to focus on where the problem occurred in order to fix it.

ERTC, I do not have the data in front of me on what type of fraud existed there. I do not think the Employee Retention Tax Credit, which is pretty important and it is still going out in important ways. And I agree with my colleagues on both sides of the aisle that these were very important. I mean, we could have gone into a depression if we shut down businesses and did not fund them to keep their employees. I mean, we would have had serious problems. But on the same note, the level of fraud.

So you know, they say that an acceptable level of fraudulent activity could be 2 to 3, even 4 percent. You know, in my business, and I probably had no business being in charge of our credit department, but we had AR at any given time at about $50, $60 million and we did not write off bad debt. It was never higher than 1 percent. And we were not all that sophisticated. So the idea that this occurs is crazy. So I think crazy.

Now, on the same note we have the IG coming in telling us that there is, what was it? I forget his numbers right now, $240 billion in fraud? And then the SBA administrator tells us it is, no, it is $50 billion. I mean, well, that is a pretty wide spread of discrepancy. So that is also highly troubling.

So back to Ms. Miller, your idea of the centralized antifraud. Look, the credit card companies, the banks do it. Why can't the SBA do it?

Mr. Breeden, I will start with you and just go right down the line. What should we be doing? Can we put you in charge perhaps?

Mr. BREEDEN. I am not sure I would.

Mr. MEUSER. It is worth the money by the way; right? With the type of billions and billions that we are talking about.

Mr. BREEDEN. Certainly having someone in charge of going after it, going after the monies that have been stolen is a great idea. I do not know that it ought to be any one person as opposed to a lot of people's job. It is a task too big for any one person. I am not sure creating a new bureaucracy in government is really going to solve the problem. The ones that we have already have not solved it. So we have to understand that if you are going to have free markets, if you are going to have a capitalist economy there is going to be fraud. If you have a socialist economy there will be fraud, too. So we have to build antifraud protections into everything we do and be aware that there have to be limits on how many businesses we shut down, how fast we want to help people, things like that if we do not want the fraud to get out of control. But right now we have a problem of getting after the people before the money is all gone.

Mr. MEUSER. All right. So collections enforcement.

And what about prevention, Mr. Taylor?

Mr. TAYLOR. Thank you, Congressman.

It is about identify verification at the front end before these types of benefit programs go out. Implementing the IAL2 standard

issued out by NIST is the first step. And being the fact that that is a government solution that should be a nonpartisan issue.

Mr. MEUSER. Absolutely.

Down the line? Thank you.

Mr. ZERBE. Congressman, I want to reemphasize something that has kind of been lost. Let me make sure you all understand a couple of facts about fraud.

The IRS does root canal audits on people. When they do root canal audits they only find offshore accounts in 7 percent—legal offshore accounts in 7 percent of those audits. The number one way the IRS finds fraud in offshore accounts is whistleblowers. Study after study shows the number one way that you find fraud is whistleblowers. And with all due respect to just say, well, we are going to depend on the SBA folks, they are doing good work, but if you want to find fraud, the way the private sector finds fraud is they have whistleblowers. The way the government is finding fraud is through whistleblowers.

Mr. MEUSER. I yield back, Mr. Chairman.

Chairman WILLIAMS. The gentleman's time is up.

I now recognize Representative Gluesenkamp Perez from the great state of Washington for 5 minutes.

Ms. GLUESENKAMP PEREZ. Thank you, Mr. Chair.

Mr. Zerbe, I appreciate those sentiments.

You know, I think that people want to build a government. You cannot legislate good behavior. Good behavior comes from the heart. You can penalize bad behavior. You can incentivize good behavior. And I think we have really in the Committee hearing today sort of beat to death this thing of we need to go after the bad guys. And it is costing us to not do that.

But I really appreciated in your testimony, Congressman Breeder that—Breeden, excuse me—that normal people, small business owners not having the time and the capacity to understand the bureaucracy of a government that is no longer operating at a human scale. So you just walk into this pit and fall through a problem and then there goes your livelihood. And so I really appreciated your pointing out putting things in plain English. What are the eligibility criteria? Can you read this if you have a reading disability? Or you know, and who is doing that work?

So I wondered if you could speak to how that was built in.

Yes, sir. Thank you.

Ms. BREEDEN. Thank you, Congressman.

I think that is terribly important. One of the things that we focus on as part of antifraud protections in every victim trust we do is to make sure that the communication of eligibility standards is as clear as you can make it. All Madoff Victim Trust. The plan was not written by a bunch of lawyers and a bunch of boilerplate. It is in frequently asked questions plain English because there are a lot of people who might file a mistaken application or one that they are not eligible for but they do not understand that. So take that part of it off the equation.

Ms. GLUESENKAMP PEREZ. Right. And it is who is at the table when these rules are being written. You do not have normal people. You have a Congress built out of a bunch of frankly lawyers

and people who have grown up in it and not the people who might be applying for these programs. And I think that is a real flaw.

Mr. BREEDEN. Yes. But the laws can be complicated. But when you have a program that is going to make loans that has eligibility standards that is where either an agency itself or in cases we do, the private sector, you spend a lot of time trying to write very clearly so people understand what is required and what is not allowed. It does not mean people will not go ahead and violate it.

Ms. GLUESENKAMP PEREZ. Sure.

Mr. BREEDEN. There will be some.

Ms. GLUESENKAMP PEREZ. But we need to make it as easy as possible for people to do the right thing.

Mr. BREEDEN. I completely agree.

Ms. GLUESENKAMP PEREZ. So thank you for that.

And you know, Ms. Miller, I also likewise appreciated your testimony. We had Inspector General Ware come in and testify a few months ago about the incredible work his office is doing to investigate these cases of potential fraud and recoup the stolen money. At the same time he shared that his office had identified 90,000 actionable leads and that his office needs more resources to investigate these leads and the DOJ needs more funding for attorneys to prosecute these fraudsters. Ninety thousand sure feels like a lot to me. It feels like he has got a lot on his plate. And I am wondering, you know, we are staring down the face of a shutdown here, so how is that going to affect the oversight in law enforcement communities' ability to crack down on fraud? And is the government losing out on money that we could be recouping would you say?

Ms. MILLER. I mean, for sure. In short, he is going to lose the time of all the people who could be doing those investigations when the government shuts down.

Ms. GLUESENKAMP PEREZ. Yeah. Yeah.

Thank you so much to all of our witnesses for being here. And thank you, Mr. Chair. I yield back.

Chairman WILLIAMS. All right. Next, I want to now recognize Representative Stauber from the great state of Minnesota for his 5 minutes.

Mr. STAUBER. Thank you very much and to all the witnesses, thanks for being here.

Ms. Miller, congratulations on being a Member of our Olympic team. I was an aspiring Olympic athlete. I was not good enough to make the Olympic hockey team but I gave it my best shot. I always wanted to be an Olympic athlete. That was a goal of mine.

I will say this, Mr. Taylor, Mr. Meuser just asked you what is the biggest thing to stop fraud and your answer was identity verification; correct?

Mr. TAYLOR. That is correct, Congressman.

Mr. STAUBER. Just changing gears here and then I am going to get back to our subject. Would that be considered in the same light for our national elections?

Mr. TAYLOR. Identify verification could go for any type of program, Congressman.

Mr. STAUBER. Thank you.

Ms. Miller, with your experience, what do you think is the monetary amount of fraud that someone should go to prison for?

Ms. MILLER. I do not have experience to make that decision.

Mr. STAUBER. Any idea? Any guess?

Ms. MILLER. No.

Mr. STAUBER. Would it be 50,000, 100,000?

The reason I am asking this is, this fraud was put on the American people. And there are people that did not get EIDL loans that should have got it. And there are people that struggled to get PPP loans in a faster timeframe and did not. And it was taxpayer money that went out.

Does anybody have an idea? Any of the other three witnesses to my question to Ms. Miller? What should be the amount somebody should go to prison for, for stealing the taxpayers' money? What is it? Mr. Breeden?

Mr. BREEDEN. Sir, I think the threshold of what can be prosecuted should be fairly low. The theory of broken windows in law enforcement that just because somebody only broke one window, if that happens across an entire city it can have a very bad effect. So the level ought to be low. Then you have to have prosecutorial discretion where prosecutors have to look at it and say is this an egregious fraud or is it not?

Mr. STAUBER. The broken windows theory as a former police officer I subscribe to that theory. Absolutely.

You know, in Minnesota we had Feeding our Future. It was a nonprofit meant to feed people. There were over $250 million of COVID-19 federal funds that were stolen. And these fraudsters bought luxury cars, real estate, and other unlawful futures. The Small Business Administration, I think, and our government, and our Inspector General, we need to hold these people to task. If we are talking about millions and millions of dollars, and Ms. Miller mentioned earlier in her testimony that some of these identify theft folks, we are not going to get the money back. To me, I understand, I mean, the broad spectrum of the fraud. But we need to make a statement as a country. This is taxpayer money. And I guess a certain percentage is expected but we have to go after it. We have to go after it to make the statement. Nobody should steal the U.S. taxpayers' money. And they did it during a pandemic when our nation was brought to her knees. That is just simply wrong. And so the experience that you all have shared with us, there is so much knowledge here.

Mr. Breeden, I think that you being in the private sector, you had mentioned a couple minutes ago that you are not a government employee and you are doing really good work. I do not necessarily subscribe to another government group or another Committee. The private sector here has shown the way. We just have to listen and give you the authority and the ability and the staff to do what you do best. Obviously, the SBA has failed here. There is no question about it.

I want to thank you for your testimony and just your years of experience. We need more of this. And this is a bipartisan issue that we need to work on.

Mr. Chair, I yield back.

Chairman WILLIAMS. The gentleman yields back.

I now recognize Representative LaLota from New York, the great state of New York, for 5 minutes.

Mr. LALOTA. Thank you, Mr. Chairman. The great state of New York, sir.

Chairman WILLIAMS. Got it.

Mr. LALOTA. Two hundred billion dollars. Two hundred billion dollars. Lets put that in perspective.

If Congress had that $200 billion back we could give the average taxpayer a $2,000 tax cut. Or we could defer conflict with China by buying four new aircraft carriers, eight new submarines, and 27 new Navy destroyers. Or we could fully fund the state and local tax deduction which a lot of my constituents would like. Two hundred billion dollars. Approximately one in five COVID loans were potentially fraudulent. Thank you, Chairman, for hosting this important meeting and shining a spotlight on this important issue that my constituents care a heck of a lot about. And for our witnesses for being here to help inform our Committee on this issue.

Despite the widespread fraud, the SBA has downplayed the fraud stolen from our fellow taxpayers and has given a free pass to anyone who has stolen less than $100,000 by refusing to investigate those smaller loans. The SBA's disregard for this issue is exemplified by the administrator's failure to testify before this Committee's July hearing with the Inspector General. It is our job on this Committee to fight waste, fraud, and abuse in the Small Business Administration, and that job is made much more difficult when the SBA administrator does not show up.

That leads me to my first question. Mr. Taylor, sir, in an effort to expedite funds, the SBA did not check the "do not pay" lists before sending money out. Is that a normal procedure?

Mr. TAYLOR. The self-certification allowed by SBA at the beginning of the pandemic was totally uncalled for and unprecedented.

Mr. LALOTA. And what is the effect on not doing that diligence?

Mr. TAYLOR. The massive fraud that we are seeing today.

Mr. LALOTA. Mr. Breeden, you have quite the impressive resume, sir. I looked it up. Harvard Law, Chairman of the SEC, and you are a native Long Islander most importantly. So that well qualifies you to be on this panel.

My question, sir, is what effect does the SBA's decision to not investigate those smaller loans have on future behavior?

Mr. BREEDEN. I think it is very deleterious, sir. It sends a message that, okay, you can play around the edges and people just will not bother. And I think the principle that if you steal from your neighbors, you steal from your fellow citizens, that will always be a matter worthy of government's attention is the right message to send.

Mr. LALOTA. It is a behavioral thing, right, that if folks know there are consequences to their negative behavior they are less likely to conduct that negative behavior; no?

Mr. BREEDEN. Yes, sir.

Mr. LALOTA. Mr. Taylor, back to you, sir. I know that we talked a little bit about Barbie before. We are going to do it just shortly once again.

How can the private sector help to identify, to do identify verification better to help prevent fraud?

Mr. TAYLOR. Thank you, Congressman.

Getting back to the Presentation Attack Detection that I was mentioning to the previous congressman about, that would have stopped those types of attacks on those Fintech platforms.

The fraud that was experienced specifically around the PPP, the top 12 lenders around that were all Fintech platforms. They would have allowed something like that to go through. Currently, identity verification, whenever you implement liveness detection at the IAL2 that is approved by NIST, it stops that in its tracks. Additionally, SBA OIG, specifically IG Ware talked about it the last time that he was here, talked about the overlapping of IP addresses and suspicious IP address activity, if this was 5 years ago that is an effective way to go about doing an investigation. It no longer holds that value at the IP address level. You have a to get into the big data that is associated with that IP address as well as the device intelligence associated with it.

Mr. LALOTA. So doing things like that obviously come at a cost; right? That it takes more to invest in better technology, better process. That comes at a cost. Would you assess that as positive ROI, is the return on that investment positive for the taxpayers? If we go through that diligence, raise the bar, do better identify verification, do we have less fraud? And is the less fraud worth * does it give us extra money to pay for those costs, sir?

Mr. TAYLOR. Yes, sir. As a matter of fact, everywhere that ID.me has been implement across 27 states during the pandemic, fraud rates went down. The pass rates went up. So it is a matter of inclusivity in these programs. It is a matter of stopping the fraud in its tracks. And also, the false positives associated with misidentifying an individual, which you can do if you are just targeting an IP address.

We are not allowed, at ID.me, we have a policy. We keep the false positive rates very low. Well below 1 percent. The fraud rates, the same thing. The fact that we are talking about programs that have 18-21 percent in the fraud rate is unheard of in the private sector.

So with that being said, I would be very cautious that any type of program that is concentrated only on the IP address. Additionally, in Puerto Rico, we took the pass rates from 23 percent up to 78 percent at a cheaper cost.

Mr. LALOTA. Thank you very much. My time is expired. Thank you, Chairman.

Chairman WILLIAMS. The gentleman yields.

I now recognize Representative Salazar from the great state of Florida for her 5 minutes.

Ms. SALAZAR. Thank you, Mr. Chairman. The great state of Florida indeed. And thank you for coming to explain to us your knowledge and everything, all the steps that you have taken.

Mr. Taylor, I hear that in the state of Florida you are able to establish a very good technique that we could replicate in the rest of the country. Could you please explain for my constituents what did we do right in Florida versus other states?

Mr. TAYLOR. Thank you, Congressman.

The relationship with Florida has been an absolutely fantastic one.

Ms. SALAZAR. Okay.

Mr. TAYLOR. We have implemented the IAL2 policy there that I spoke about previously. So the fact that when you have identify verification gating a lot of the public benefit programs there——

Ms. SALAZAR. And how does that work in particular so I can understand. I do not have a criminal mind so I am not sure what people think. Shat do you need to do in order to defraud the government? So why the facial identification is important?

Mr. TAYLOR. Less about the facial recognition side and more about the actual Liveness detection. The fact that a person is a real individual. The mask that made it through and the Barbie Swindler. Those do not make it through ID.me in the State of Florida. Because we have that Liveness detection built into the platform.

Additionally, we have unsupervised sites. So if a person cannot get through, let's say that there is a language barrier, we support over 200 languages on that side. So the person can come through, talk to a trusted referee. And we are talking about wait times that are less than 5 minutes to get onto those platforms.

Lastly, I would turn your attention to Hurricane Ian last year. The devasting impacts with that, obviously in the billions dollars and loss. We have a thread intelligent cell that lives out on the Dark Web that looks for fraudsters going after these types of benefit programs. We actively go out and look for the bad guys going after these public benefits, and we did that in the state of Florida. So much so that whenever Hurricane Ian occurred, we had the in-person terminals that the IME has, and the people were able to verify their identity, get their FEMA funds right there in the spot instead of having to wait in line to go to a state office or something like that.

Ms. SALAZAR. So the facial identification could be the answer for the federal government to stop future fraud across the board or across the nation. Would you consider——

Mr. TAYLOR. It is one part of an entire fraud suite of tools that we would recommend.

Ms. SALAZAR. Explain to my constituents why after the pandemic we had so much fraud. I would imagine that people were claiming that they could not find work or that they did not have a job. Explain to me the scenario after COVID.

Mr. TAYLOR. During the first 9 months of the pandemic you had self-certification of these benefit programs. Combine that with the speed at which they were decimated, you are talking about an unprecedented amount of capital that went out into the economy. That incentivized a lot of nation state actors, as well as your traditional domestic fraudster to go after these benefit programs.

Ms. SALAZAR. Okay.

Mr. TAYLOR. Your constituents have not only suffered from the standpoint of losing your identity, possibly for tax purposes or filing for unemployment but also they may have inadvertently had their identity used in a credit scheme that would target a small business.

Ms. SALAZAR. Okay. So we know that the SBA, there is a dispute of the amount of money that went to the wrong hands through the PPP program. Do we have a figure of how much money went to the wrong hands? Or how many millions of dollars were lost after the pandemic for claims from people that did not deserve or

were not the right beneficiaries of these monies for unemployment benefits?

Mr. TAYLOR. Thank you, Congressman. I would agree with IG Ware that the likely fraud is somewhere in that realm of $650 billion. The fraud number right now that he is planning on going and prosecuting at 200 billion.

Ms. SALAZAR. Two hundred billion dollars. And this money that we are talking about is included in that figure of 200 billion?

Mr. TAYLOR. That is correct, Congressman.

Ms. SALAZAR. Okay. Thank you. I yield back.

Chairman WILLIAMS. Next, I now recognize Representative Phillips from the great state of Minnesota for 5 minutes.

Mr. PHILLIPS. Thank you, Mr. Chairman. Thank you for holding this hearing, and to all of you for being with us.

Let me just start by saying I share every one of my colleagues' disgust by the scale of fraud that took place during the pandemic, and we have got to do everything we can to investigate and most importantly recoup billions of dollars that were literally stolen from American taxpayers. Stolen during what I consider a tragic moment in our history.

The good news in my estimation is that we have got a clear roadmap, and that is to give the SBA Inspector General the resources that his office needs to go after these fraudsters.

I come from a business background myself, like the Chairman, where return on investment is the name of the game. The IG's office has requested $47 million in discretionary funding for its operations in fiscal year 2024. Unfortunately, the House Appropriations Committee underfunded that request by about $15 million. Yet, over the past 2 years, OIG's efforts have yielded over $9 billion in financial accomplishments, recoveries, fines, and forfeitures. Considering these numbers, an extra $15 million in my estimation seems like a heck of a good return on investment to me. Inspector General Hannibal Ware has proven that his office delivers results for taxpayers and Congress simply needs to give him the tools to do his job.

So I would welcome suggestions from our witnesses today. And we ought to consider them fairly, but we cannot lose sight of the fact that the number one thing we can do to recoup fraud is to fund the Inspector General's office fully.

Let me just start with you, Mr. Zerbe. I really appreciate the bipartisan tone in your testimony. I think you are right, that eliminating fraud, waste, and abuse of the SBA is a bipartisan exercise. Must be bipartisan. In the same way that small business relief was. I am intrigued by your proposal to establish a whistleblower program at the SBA. It has proven successful at other agencies, of course. But one of my concerns is that the IG currently lacks resources to actually investigate what I think are about 90,000 actionable leads that it has already identified.

So what do you make of this concern?

Mr. ZERBE. Thank you for that, Congressman.

I think a couple of thoughts for you. One is that I agree they have got kind of a fire hydrant drinking moment right here but I still think that the whistleblowers will be able to: (a) better target the most important fraud cases, and also just so you understand,

when you are submitting, particularly when you have an award program, it is not just a tip and things like that. The whistleblower and his attorney, they are providing a whole package for the agency. I mean, we are putting in the documents, the material, a view of the law, a narrative. We want it on a T-ball for them to be able to just do it. So it is making the agency much more time efficient and effective in terms of what they are doing.

One thing, too, to consider and you might think about as you are looking at legislation in this area, it is not uncommon for the whistleblower award programs and the Qui Tam programs in other agencies to allow for a reimbursement of the costs the agency has with their investigation as well, too. In other words, yes, we recovered these funds, and yes, you know, we are going to reward the whistleblower. But we are also going to reimburse the SBA for its costs as well, too. So it may be something to consider to address the concern you have got about limited agency resources to say, great, we are going to in a sense incentivize not only the private sector to come forward and assist the SBA through the whistleblowers but we are also going to incentivize the SBA to embrace those whistleblowers and work with them because then they will basically be able to have their costs met. So that may be a way to address your concerns, Congressman.

Mr. PHILLIPS. And based on that absurdly high number, 90,000 leads, are there alternatives concerning the resources, levers, tools we have available to us? In your estimation, are there other mechanisms we should be considering to reduce that workload and ensure that every one of those leads is investigated?

Mr. ZERBE. Well, I think that is where it is going to help not to repeat. But I think having seen a lot of these kind of tips, particularly more from my IRS work, a lot of them tend to be pretty thread bare. I mean, just, well, you know, Jimmy has got a fancy car and you guys should go look at him. I think, you know, when you are getting the whistleblower you are getting an insider informed and you are getting the big fish. So the SBA——

Mr. PHILLIPS. Okay. So quality, not quantity?

Mr. ZERBE. Yeah. And the IG white paper highlighted one. They had one whistleblower who came forward and it was over $600 million that they had identified thanks to this one whistleblower. So you are right. It is able to get the big fish and the worst actors, if you will, and target them better on that. Yes, Congressman.

Mr. PHILLIPS. Okay. I appreciate it. I have only got about 20 seconds left.

I just want to refer to a letter that I plan to send to both the House and Senate Appropriations Committees requesting that they fulfill the OIG's full request of $47 million in discretionary funding because holding these bad actors accountable should be bipartisan goals, and I surely invite my colleagues on both sides of the aisle to join me in that endeavor.

With that, Mr. Chair, I yield back with exactly 1 second left.

Chairman WILLIAMS. Great job.

I would like to thank our witnesses today for their testimony and for appearing before us.

Without objection, Members have 5 legislative days to submit additional materials and written questions for the witnesses to the Chair which will be forwarded to the witnesses.

I ask the witnesses to please respond promptly.

So if there is no further business, without objection the Committee is adjourned.

Thank you all very much.

[Whereupon, at 11:35 a.m., the committee was adjourned.]

APPENDIX



Committee on Small Business

U.S. House of Representatives

Hearing on Private Sector Solutions to Recouping Stolen Pandemic Loan Funds.

Testimony of the Hon. Richard C. Breeden

September 27, 2023

I am honored to appear before you today as you consider the appropriate response to widespread instances of fraud in connection with Covid-19 EIDL and PPP Loans of the U.S. Small Business Administration ("SBA"). We have more contentious differences in our national politics today than when I was privileged to serve under Presidents Ronald Reagan, George H.W. Bush and William Clinton. However, hopefully most of us can agree that it is wrong for anyone to commit deliberate fraud against our neighbors and fellow citizens.

Fraud and dishonesty are perils in any economic system. Large pools of money attract people determined to take as much as possible, even if they are not eligible. Left uncontrolled, fraud and looting of lending programs can grow to dimensions that damage the broader economy and discredit whole sections of markets. The savings and loan crisis of the 1970s-1980s, the subprime mortgage and banking crisis in the early 2000s and the fraud on COVID lending programs of the past few years all grew to the point of doing devastating harm. Large frauds involving private companies such as Enron, WorldCom, Madoff and others can also destroy companies, the jobs and security of their workforce and their families and the savings of those who invested in them.

By whatever measure one uses, an enormous sum - as much as $200 billion or more – was stolen through fraudulent loan applications to the SBA that were not detected by SBA or its contractors. In preparing this testimony I reviewed the *White Paper Report* dated June 27, 2023 of the Office of Inspector General of SBA (the "OIG Report"), and also the Report of the Government Accountability Office ("GAO") to Congressional Committees entitled *Covid Relief: Fraud Schemes and Indicators in SBA Pandemic Programs* (the "GAO Report"). Both reports establish without doubt that the pandemic-era loan programs of SBA experienced an epic level of fraud.

Those who deliberately stole public funds should face a day of reckoning. Strong efforts to recover stolen funds are warranted for many reasons. I hope that I can contribute to your

efforts in considering how private sector solutions can assist in recouping stolen loan funds and in doing a far better job of preventing recurrence of these problems. At the outset, I would like to summarize briefly my experiences in the public and private sectors that form the backdrop for my testimony.

I. Background in Antifraud Efforts.

White House Service.

In January of 1989, savings and loan and other "thrift" institutions[1] held roughly $1.2 ***trillion*** in federally insured deposits from the public. After years of heavy losses, the Federal Savings and Loan Insurance Corporation (FSLIC), the analog of the FDIC for banks, was down to roughly $3 ***billion*** in remaining cash to back its insurance. It had the ability to borrow less than $1 billion from the Treasury. There were dozens of very large thrifts that were hopelessly insolvent, and which could have taken down the deposit insurance fund in a morning. President Bush did not particularly relish dealing with savings and loans in his initial days in office. However, he was adamant that he would not allow the country to default on promises to insure the savings deposits of tens of millions of citizens.

Approximately three weeks into his tenure in office, President Bush proposed legislation to Congress to finance closing insolvent institutions and protecting every insured depositor. The legislation, which became known as FIRREA, authorized the issuance of special purpose bonds to finance paying cash to the insured depositors. The legislation also created a new agency called the Resolution Trust Corporation ("RTC") to acquire, manage and sell **hundreds of billions in assets** that had belonged to the failed firms. RTC was a gigantic SWAT team for troubled assets that had previously backed defaulted loans made by the thrifts.

With an historic flood of troubled real estate that needed to be sold to recover taxpayer money, we believed this task could best be handled by people with the skill and experience in selling real estate in large blocks. We didn't want to sell one building at a time. Rather, we wanted to sell balanced portfolios containing numerous buildings at a time. Bank regulators don't have those skills, and liquidators at the FDIC didn't either. So, President Bush decided to create a new temporary entity[2] to launch a *blitzkrieg* against the toxic assets and turn them into cash.

---

[1] This was a term that generically referred to savings & loan firms. It included mutual savings banks and other institutions originally developed in the mid to late 1800s to promote savings and thrift by citizens of ordinary means.
[2] FIRREA was passed by large bipartisan majorities. It mandated that RTC would go out of business once it completed the recycling of thrift assets. This avoided creation of a new permanent agency.

RCB Fund Services

After some initial growing pains, the RTC collected hundreds of billions from the assets of the failed thrifts in a very short time. This was accomplished mostly by drawing on private sector firms to help package and sell troubled real estate and other assets, rather than trying to create a permanent bureaucracy to do so.[3] Wherever possible, RTC retained a participation in the value of the portfolios as they were liquidated.

In addition to creating RTC, President Bush believed that it was important to take strong action against individuals who had engaged in wrongdoing associated with failures of some institutions. We believed that unknown billions in loans had been made based on loan applications that were partially or entirely false. Also, some real estate developers had acquired control of thrifts and then made loans to themselves with blatant conflicts of interest.

To address this issue the legislation included funding to create new task forces of investigators and federal prosecutors. It also toughened the legal standards of what constituted fraud on federally-insured institutions, and increased sanctions. Even though we knew there were long odds against these actions, the President believed that the public should know that we exerted maximum efforts to hold fraudsters and looters accountable.

Thus, our overall effort was a two-pronged attack on the legacy of fraud. RTC pursued every commercial avenue for selling the assets of failed firms in a commercially sensible manner, and without warehousing billions in properties in government hands. At the same time, the Department of Justice pursued criminal sanctions against those who had committed fraud.[4] While I am admittedly biased, I believe that the bipartisan efforts of the President and Congress that resulted in the savings and loan recovery bill averted a financial apocalypse and immensely benefitted the public.[5]

Service at the U.S. Securities and Exchange Commission (1989-1993).

In October of 1989, President Bush nominated me to serve as Chairman of the U.S. Securities and Exchange Commission ("SEC"), where I served for just under four years. Combatting fraud against investors is one of the SEC's preeminent responsibilities, and during my tenure we brought over 1,200 enforcement actions. A great many of those actions were targeted against

[3] Private sector resources were important in the RTC's efforts. However, not all private sector entities proved successful. Not entrepreneurially focused, law and accounting firms lacked expertise in selling real estate or other recovered assets, and their astronomical fees ate up recoveries quickly. There is a similar problem in many bankruptcy proceedings involving fraud, where legal fees can eat up most of the potential recoveries for fraud victims.

[4] In hindsight, we missed an opportunity to do even more by not making forfeiture actions a more important part of our arsenal. In my experience, forfeiture actions are by far the most effective tool in recovering funds related to fraud, and redirecting those funds back to the victims of crime or to the taxpayers.

[5] In contrast, the TARP program in the subprime crisis was far less well thought-out in my view, and relied more heavily on discretionary assistance actions that were not always consistent with accountability.

persons who had committed fraud in various forms, including falsification of financial statements.[6]

My SEC experience taught me many lessons about the tools required to successfully combat fraud in the market. Fraud -- an intentional use of dishonesty to acquire funds – comes in an almost infinite variety of forms. It can involve false statements, false documents and almost any other type of falsehood. Something that is one thing is made to look like something better. Sometimes a fraud uses information that is partially correct. Other times, such as in a Ponzi scheme like Madoff, ALL information is false. Sometimes a fraud can be small in scale, and in other cases like WorldCom, Madoff, or false PPP and EIDL loans, the scale is enormous. As a result, combatting fraud effectively requires people with years of experience, backed by good surveillance and prosecutorial tools.

One element in blocking marketplace fraud is effective surveillance to detect situations that may indicate that fraud or market manipulation is ongoing. Sometimes indications of a fraud are readily apparent, such as when market prices suddenly spike or plunge without apparent economic cause. Other times, signs of an ongoing fraud may be subtle and very hard to detect. Effective surveillance requires good monitoring systems that are sophisticated enough to identify anomalies, and that do so in real or near-real time.[7]

My SEC experience also showed me how critical it is to have a well-trained and alert staff. In the 1990s, the SEC discovered what was then the largest Ponzi scheme in history because a staff attorney thought something in a newspaper article sounded strange. The article in question described a privately-held equipment leasing company that claimed it had won a contract to lease $100 million in copy machines to the New York City Transit Authority. The company was selling those leases to investors. The staff member calculated that at an average price for a machine, the transit agency would be acquiring more than 12,000 copy machines in this one transaction, which would have required several on every bus. An inquiry was started, and the SEC eventually discovered that the company had sold or financed $2.5 billion in nonexistent leases. In another case a staff member read an article about a rapidly growing local

[6] The use of inaccurate financial statements in the sale of securities is a "fraud", if it was done deliberately. If an intent to defraud was not present, inaccurate financial statements may still be false and misleading to others. Though there are cases where financial statements used to raise money from investors (or lenders) are inaccurate due to errors in preparation, in most situations where money is obtained through false and inaccurate financial statements, the inaccuracies are deliberate. For law enforcement, proving fraud is much more difficult, since it involves a state of mind, than proving that financial information was inaccurate or misleading.

[7] While the quality of surveillance systems is very important, it is easy to overstate their role. All too often, people assume that "Big Data", "AI", advanced algorithms or some other technological marvel will find fraud all by itself. In my experience, technology is a vital tool for regulators and investigators. However, sitting around waiting for Big Data to find a fraud is likely to be disappointing. Frauds are usually found by people who have the experience, diligence and insight to challenge something that looks unusual, or to follow up on complaints from individuals reporting a problem.

Maryland company holding investment meetings in local churches. The staff person inquired about investing and received in the mail a "pitch" for a rapidly growing affinity fraud promising minority investors returns of 25,000% in six months. Because of that alert individual's rapid action, we were able to shut down a rapidly growing scam.

Fraud is often first uncovered by victims, or by people inside a company who may witness something they know is unusual or suspect. Early complaints sometimes get brushed aside as not credible. However, tips or complaints are often the first and best indication that fraud is taking place, and it is vital that they be reviewed carefully. The audit committees of large public companies usually have an Ethics Hotline or other system for enabling employees to report information about wrongdoing in the company directly to the board. ***Qui Tam*** suits and formal whistleblower programs such as the IRS and SEC use are other techniques for giving individuals a monetary incentive to come forward to the government with information they possess about improper conduct.[8] Once a company or a government agency is alerted, it will hopefully follow up to determine if something that appears normal is really a sign that fraud is occurring. In part that depends on the organization having a culture of truthfulness and accountability so that tips are not just ignored.

In cases of fraud, the SEC almost always goes after the money stolen from investors or others. One traditional type of litigation was to seek "disgorgement", which is to recover the profits made by someone who engaged in unlawful or improper conduct. Disgorgement is similar to forfeiture actions Congress has authorized in connection with many other types of criminal actions with the intent of taking away the profits from crime.[9] In the early 1990s, Congress gave the SEC authority to fine individuals or companies for violating the securities laws where disgorgement wasn't an adequate remedy. Fines are useful where the harm from an unlawful practice far exceeds the profits made by the person or firm engaging in unlawful conduct.

Once the SEC learns of a fraud or other improper or unlawful conduct, its Enforcement Division brings civil litigation against the persons or companies that were involved. Similarly, U.S. Attorneys and DOJ often swiftly bring forfeiture actions to recover against large criminal wrongdoing. In the Madoff case, the DOJ recovered over $9 billion through forfeiture suits, enabling victims to recover a very large portion of their fraud losses. Historically the SEC has used its own internal resources to seek to recover stolen funds, rather than partnering with the private sector which would be fraught with conflicts of interest and other issues. However, to

[8] The SEC did not have a "whistleblower" reward program when I served as Chairman. One must be careful that incentives for reporting misconduct do not become so large as to incentivize misreporting.

[9] In my opinion, forfeiture actions are the most powerful and efficient tool for attacking fraud and recovering funds for victims of unlawful activity.

some degree the SEC partners with the private sector by encouraging companies to "self-report" violations in return for lighter sanctions.

Strong internal controls against fraud are vital for public agencies like the SEC and SBA, as they are for large publicly traded companies. Under Section 404 of the Sarbanes-Oxley Act, publicly traded companies are required to have effective controls against fraud. The CEO and CFO must personally certify that the information contained in an SEC filing is accurate, and the company's internal controls must be audited by its public accounting firm. The private sector has expended enormous effort and expense in developing frameworks for acceptable internal controls against fraud over more than 30 years backed by capable internal audit teams. These efforts include the development of the "COSO" antifraud principles and numerous auditing standards promulgated by the SEC and the accounting profession.

As frauds at Enron, WorldCom, Madoff and many other companies show, even good controls can be overridden by persons orchestrating a fraud. In WorldCom, executives in the accounting and treasury functions might come to work and find a sticky note on their computer screen from the CFO telling them to add $300 million or some other large figure to revenues in a particular area. In those situations people did what they were told. Some later explained that they assumed that the CFO was aware of consolidation or other issues with other parts of the company that they weren't familiar with. Unfortunately, WorldCom's internal auditors, its independent external accountants and its board of directors did not detect that management was inflating reported revenues and profits every quarter for several years. When it restated its financial statements, roughly 75% of WorldCom's pre-fraud reported assets were eliminated, and over $15 billion in reported earnings proved non-existent.

Administering Trusts and Other Funds for the Benefit of Victims of Unlawful Conduct.

In the private sector, I have administered a series of trusts, bankruptcy estates, Fair Funds or remission funds on behalf of Federal courts, the Department of Justice or the SEC. Set forth below is a partial list of these engagements:

- The Bennett Funding Group (Bankruptcy court)
- WorldCom/MCI (Federal Court)
- Enron (SEC Fair Fund)
- Shell Oil (SEC Fair Fund)
- British Petroleum (SEC Fair Fund)
- JP Morgan Chase (SEC Fair Fund)
- Adelphia Communications (DOJ forfeiture fund)
- Madoff Securities (DOJ forfeiture fund)
- General Electric (SEC Fair Fund)
- Facebook (SEC Fair Fund)

- Kraft Heinz (SEC Fair Fund)

These entities exist to administer payments to the victims of unlawful conduct that depressed or destroyed the value of a company's shares, or that led to a company's collapse. Many of the companies that violated the law remained in business, while others collapsed. In each case there is a written plan of distribution that sets forth the eligibility standards for a recovery (like the eligibility standards for an SBA loan). Applicants for funds have to submit a claim or petition that demonstrates they meet all eligibility standards. They must also document the amount of their fraud loss through financial records and other documents. My team and I then review all claims so we can recommend which should be approved, and in what amount.

In many respects, administering such a fund is a smaller version of administering PPP or EIDL loans. In each case there is a limited pool of funds available for helping a defined group of eligible recipients. The plan of distribution approved by a Federal court or the Justice Department, spells out the criteria for eligibility, as well as how each person's losses will be calculated. We publish notices of the existence of a fund and set up electronic and physical filing mechanisms that applicants use. Documentation from claimants covering millions or tens of millions of transactions involves voluminous data that must be analyzed both for eligibility and for loss calculation. I believe this work is similar to reviewing data regarding employees, payroll, benefits and other issues in connection with PPP/EIDL eligibility and loan amount.

The fraud cases that I have administered were all very different. There were large and small cases in terms of the dollar size of the fund. Some cases were widely known and attracted huge numbers of claims, such as WorldCom, Enron, Shell Oil and GE with over 2 million claims collectively. Other cases involved less well-known companies and/or much smaller numbers of claims. Each case had its own unique facts that affected the claims. WorldCom, Enron and Madoff all involved cases where equity investors lost every penny when the companies collapsed. Shell Oil, British Petroleum, JP Morgan and others were cases where false disclosures caused losses to shareholders, but the companies and their share prices eventually recovered.

Administering these victim trusts is not so dissimilar in important respects from reviews that had to be made for PPP/EIDL loans. Both our cases and SBA's involved two essential decisions that had to be made through an application process. These were (i) whether the applicant met eligibility standards for a loan, grant or payment, and (ii) how much was the individual entitled to receive. Each program requires documentation to demonstrate eligibility for a loan or for a payment, and to verify the amount. There are enough similarities in the two types of programs that there are several observations from our 20 years of work with these trusts in the private sector experience that the Committee might find useful.

RCB Fund Services

First. The dollar amount of false, ineligible, duplicate and overstated claims (collectively, "false claims") has been very substantial in every large case.[10] The SBA's experience of large volumes of false claims is not an aberration because it was a new program. Rather, large numbers of false claims must be expected and controlled in any government grant or loan program if taxpayers are to be protected. The ocean is always wet, and government grant and loan programs always attract individuals willing to make false and overstated claims.

My team and I have reviewed approximately ***4 million claims*** of loss involving roughly ***140 million*** securities transactions. We reviewed claims with total claimed losses of over ***$170 billion*** dollars. **After thorough scrutiny, we have found that eligible and properly documented claims generally constitute from 30-70% of the dollar amount of claims received.** Thus, after carefully reviewing claims involving $170 billion in claimed losses, we have only recommended approximately $45.5 billion of those claims.[11] Even assuming future approvals, we will not reach $50 billion in approved claims, or an approval rate of less than $1 out of $3 in claims. Thus, in our experience, which spans 20 years of work, waste, fraud and abuse would have misdirected as much as 2/3rds of available dollars into the wrong hands if we hadn't stopped that from happening. In doing our reviews of claims, we regard ourselves as being the people who make sure that the money originally won by the government actually reaches the victims of unlawful conduct that it was intended to help.

Second. There has not been a single case without significant numbers or dollar value of false claims. The highest percentage of dollar amount of claims we have ever been able to approve in a major case is 73%, with 27% denied. However, even in the case with the highest dollar approval percentage, there were still false claims of more than $1.5 billion.

Third. Without a rigorous review, false claims in large numbers will be approved, resulting in horrific losses to taxpayers and the public. Analyzing large volumes of claims with detailed eligibility standards as with the PPP and EIDL loans is difficult and time consuming. Identifying ineligible or overstated claims for payment can utilize computer systems to some degree. However, technology also provides the tools for fraudsters to create perfect-looking fake documents. Therefore, finding false claims requires a multi-layer process using both experienced analysts and good systems. Sometimes finding the false and fraudulent claims is like looking for a needle in a haystack. In WorldCom, a single claim filed by an investment

[10] For discussion purposes, we do not distinguish in these statistics between claims that upon review did not satisfy eligibility criteria, or that contained false loss information, and those ineligible or overstated claims that were filed with an intent to defraud the government. Our role as administrators is to protect eligible victims from having their recoveries diluted by false/overstated claims, not to go beyond and assess any criminal liability. We have seen billions in what we believe were "fraudulent" claims mixed among over $125 billion in claims that were not eligible or that were overstated, whether due to confusion, mistake or deliberate action.

[11] Several large ongoing cases have not reached the stage of recommendations for approval or denial, and the $45.5 billion number will rise when that happens. However, the overall proportions will remain within the historic norms described.

advisory firm included seriously inflated prices on 17 transactions (out of 10 million transactions we reviewed). However, including those 17 transactions at the value the firm put on them would have overstated the firm's legitimate claim by over $2 billion if not detected. Whether deliberate or by mistake, inflated or ineligible claims need to be challenged. In another case, one of the largest financial firms submitted a $1.5 billion claim that was entirely ineligible, but that contained full documentation. The information submitted was accurate, but it only showed some of the firm's trades. By omitting complete information, the firm made a profit into a large loss and sought payments from the fraud fund.

Given the magnitude of false claims, investing in effective review systems pays an enormous return. For every dollar our firm spends on claim analytics, we typically expect to prevent several hundred dollars in false claims from being approved. Losses to taxpayers (or to legitimate victims in our case) are measured in the billions, while strong fraud detection efforts that could prevent much of the loss are measured in millions. As a matter of economics, well-executed government efforts to establish strong and effective antifraud practices will pay for themselves many times over. They should also reassure the public that tax dollars are not being squandered without reason.

Despite the benefits of strong antifraud efforts, we do not believe that there is any government-wide mandate for agencies to make fraud detection an essential part of internal review of loans or grants, or in selecting private sector contractors. Indeed, there often is a "lowest cost bid" mentality in selecting contractors through competitive bidding. Unfortunately, lowest cost bidding for administrative services (what might be called "see no evil, hear no evil" review) will almost inevitably produce the highest levels of undetected false claims.

Fourth. Where fraud is detected, it needs to be prosecuted criminally, in addition to vigorous action to recover stolen funds. If there is no price to pay for submitting a false claim, then the behavior will only multiply. Criminal actors may systematically file false claims, knowing that many will sneak through review. Even a low percentage of success can be highly profitable for false claims. Therefore, there needs to be stronger deterrence than simply denying false claims. Criminal sanctions are the most effective, but unstinting pursuit of stolen funds is also important financially and psychologically. Mansions, airplanes and exotic cars purchased with proceeds of fraud need to be taken away, ideally in a very public manner.

Fifth. The dollar amount and number of instances of serious fraud is most prevalent among "institutions" or larger firms, as opposed to individuals. This is particularly true with firms making claims relating to proprietary trading. Limiting the size of companies that could apply for PPP loans, for example, was one effective method of limiting the overstated claims that otherwise would have occurred. In our experience, the largest amount of "errors" or false claims occurs with large firms claiming funds for their own account, and with firms paid to file

claims on behalf of others. Our firm separately reviews every large proposed payout to double check validity.

Sixth. It takes time to find fraud, so necessary systems need to be created and tested in advance. One of the obvious differences between our experience with identifying false claims and PPP/EIDL was the intense time pressure SBA was under. If the necessary systems, including outside contractors, can be established and tested on ongoing activity, it will be easier to surge personnel and scale systems in the event of a larger crisis. Both the SEC and the DOJ maintain pools of firms that can handle these types of review assignments.

Seventh. Using commercial banks to process loans guaranteed by the government without accountability for loss will not work. The subprime mortgage crisis demonstrated that banks that process loans or securities and then securitize them for a fee, without retaining risk, will do so without meaningful limits. Anyone who has applied for a new bank account also understands that the depth of regulatory minutiae involved in modern banking makes nimble response to a crisis difficult to envision. Certainly the SBA needed outside assistance to handle the volume of loan processing. Turning to commercial banks as intermediaries did not seem to produce good results in blocking fraud. In many cases, banks produced computerized templates that were confusing to themselves as well as to SBA loan applicants. Review personnel may themselves have been confused, and the results do not suggest either proficiency or accountability for accuracy.

The SBA needed to keep control of drafting loan applications matched to eligibility standards. It also needed to interpret ambiguities rapidly and communicate answers to common questions effectively. Eligibility standards need to be expressed very clearly, in plain language and with examples claimants can understand. This will not prevent deliberate false claims, but it can sharply reduce the number of inappropriate claims made in good faith. In the Madoff case, for example, the Madoff Victim Fund published our eligibility and loss calculation criteria in the form of FAQs written in plain English. As we received questions from lawyers or claimants during the claim period, MVF published the incoming questions and our responses on our website to provide maximum assistance on interpretive questions.

Eighth. I am not aware of any government-wide legislation requiring every government grant or loan program to make identifying and expunging fraud and/or overstated and inappropriate claims a priority. We require agencies to conduct a cost-benefit analysis of many proposed actions, and to review paperwork burdens. We require competitive bidding for many government procurements. Inspectors General and the GAO are important voices for antifraud systems. However, I believe Congress should consider much stronger requirements for agencies to include identification and prevention of fraudulent claims at the beginning of their processes, not simply to have after-the-fact reviews as occurred with TARP and CARES. Federal law requires every U.S. publicly traded company to establish effective internal controls,

and to have its internal financial controls audited periodically. Certainly there could be stronger requirements for agencies to make fraud prevention capabilities a significant factor in hiring of outside contractors to be involved with administration of loans, grants or similar financial programs.

II. **Suggestions for Action**

The GAO's Report on Fraud Schemes and Indicators in SBA Pandemic Programs notes accurately that it is much more difficult to recover funds from fraudulent loans after the fact than it is to detect and prevent fraudulent loans at the application stage. However, at this time, recovery efforts are the only answer for improper loans that have already been made. Both the SBA OIG and GAO have already made excellent suggestions. Given my limited knowledge of the internal details of SBA's lending review and interactions with contractors, it is difficult to make informed suggestions for the Committee. However, I would suggest

1. Litigation against enablers of fraud.

My time at the SEC involved many efforts by the Commission to seek disgorgement of profits resulting from unlawful behavior. Disgorgement is a civil lawsuit to recover what are, in essence, proceeds of unlawful or unethical activity. If SBA does not have statutory authority to sue any person who submitted, prepared or reviewed a seriously inaccurate loan application that resulted in ineligible or significantly overstated proceeds, the Committee might consider giving it such authority.

Unlike the power to seek disgorgement of wrongful profits, civil fines were not originally part of the SEC's arsenal. However, in 1990, Congress authorized the SEC to assess fines for unlawful conduct. Imposing larger penalties is valuable when dealing with larger firms that have committed violations of the law or contributed to losses due to its own negligence or reckless behavior.

The OIG Report mentions that one of the lenders SBA used to process PPP loans went from a volume of 200 loans per year to almost 500,000 loans per year during the pandemic without any substantial increase in staff. If true, that would suggest reckless behavior at a minimum while the institution tried to increase fee income. Banks seem to have been the intermediaries for a very large portion of the COVID loans. At least in the future, there should be accountability for any firm that collected significant fees without meaningful efforts to identify fraudulent loans. Depending on the provisions of applicable contracts with SBA, the conduct of intermediary banks with the top 10, top 20 or top 30 dollar volume of originations might be useful to review independently. If there are firms that profited significantly from negligent or reckless behavior, recovery actions should be brought.

Individuals and entities that procured loans using fraudulent documents and other faked information should be pursued vigorously. Efforts to date in obtaining arrests and indictments are very positive. Congress contributed significantly by extending the statute of limitations to provide ample time for pursuit of wrongdoers. To the extent possible, the efforts to seek out and prosecute deliberate fraudsters should continue with utmost vigor. A vital question is the ability to develop leads for follow-up investigation and enforcement.

Many programs have had effective whistleblower programs to incentivize citizens to report wrongdoing. The guidance for applicants regarding eligibility for PPP and EIDL programs seems to have been quite confusing. Millions of applicants were firms with only a handful of employees, who may have lacked the records management capabilities of larger firms. Thus, I would personally hesitate to create significant financial incentives for "whistleblower" actions against firms employing a handful of people. However, it might be sensible to create a whistleblower type program limited to firms of more than some minimum size, such as 200 employees, for example. Since the taxpayers have been the loser with these loans, sharply limiting awards to whistleblowers might also be appropriate.

2. Forensic analysis of targeted loans.

Both the OIG Report and the GAO Report describe efforts to deploy IT solutions in identifying indices of fraud. The OIG has indicated that it has 100 years' worth of investigative work based on credible complaints and leads already in hand. This cries out for immediate and accelerated action.

I would suggest the creation of small "fraud detection teams" ("FDTs") to work with OIG or some appropriate group in SBA. In my view, FDTs should be mini-SWAT teams with no more than 50 or 100 people to avoid bureaucracy and paper-shuffling. OIG could carve up its 100 years of investigative work and assign blocks of identified loans/complaints to each FDT.

To make sense, FDTs should have demonstrated experience identifying false and fraudulent loans or grants. They should also have a short leash for proving cost effective. Retention contracts could be limited to 3-5 years with interim reviews of performance metrics. Focus should be on the largest loans, because that is where the largest improper loan amounts will be found. However, deploying a few hundred experienced analysts in an intense process should make it possible to enhance the fraud target list significantly in a relatively short time frame. Firms could be deployed by region, by industry sector, by size of firm or other criteria. Because of the waste and abuse the public has already endured, I would establish a strict budgeting regime for FDTs, including a limit on hourly fees that can be billed (such as $600) and some requirement to demonstrate identified fraud or overstated loans in excess of fees.

As noted earlier, I am deeply skeptical of the suitability of the large professional firms – law or accounting – to do timely and efficient work to identify wrongdoers. In WorldCom,

aggregate professional fees exceeded $600 million. In the bankruptcies of Lehman Brothers and Madoff, aggregate professional fees exceeded $1 billion. The bankruptcy of FTX could easily set a new record. The large New York law firm representing FTX in bankruptcy billed $400,000 per day in fees for the initial three weeks of the case, using partners charging over $2,100 per hour. Given that the COVID loans show severe waste and abuse of taxpayer funds, any outside effort to enhance the pace and scale of recovery litigation should be designed specifically to avoid the appearance of highly compensated professionals adding to the taxpayer's burdens. Since we are talking about the "small business" administration, I would suggest that smaller investigative firms should be used as FDTs.

In the Madoff case, roughly 50 individuals identified just under $70 billion in excessive or ineligible claims. Those 50 analysts identified more than 23,000 individual claims that were denied for lack of eligibility. In WorldCom, roughly 125 people were able to identify 195,000 ineligible claimants. Those 125 people blocked more than $28 billion in improper or overstated claims. In Shell Oil, roughly 125 people were able to identify 140,000 claims that did not meet eligibility standards. Over $1.5 billion in improper claims were identified and blocked. Each of these review processes occurred over a longer period of time. To some extent, the time required can be shortened by adding more individuals to the effort. However, with the fraudulent COVID loans, the goal is to sharply increase the pace and volume of recoveries, knowing that much of the damage has been done and will prove unrecoverable. During my time at the SEC, fewer than a dozen people were often used in cases seeking to recover tens of millions of dollars that resulted from unlawful acts. Therefore, I believe strongly that small FDT teams will be most effective and easiest to hold accountable for success. What is needed is an intense effort using individuals with the skill and attitudes to find wrongdoing.

I hope that these comments prove helpful to the Committee, and I will be happy to answer any questions.

Testimony of

JT Taylor
Senior Director of Fraud
ID.me, Inc.

"Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds"

United States House of Representatives
Committee on Small Business
September 27, 2023

ID.me is a Credential Service Provider (CSP) independently certified against the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 Identity Assurance Level 2 (IAL2), and Authenticator Assurance Level 2 (AAL2). ID.me is able to verify users via omni-channel pathways, including Unsupervised Remote (online self-serve), Supervised Remote (video chat), and in-person options. ID.me supports over 113 million users and more than 650 private sector partners, including 15 federal agencies and 36 state agencies. Of the 113 million users, over 48 million have active NIST credentials.

JT Taylor
Senior Director of Fraud
ID.me

Chairman Williams, Ranking Member Velázquez, and Members of the Small Business Committee: I am honored to be here today to present testimony about *Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds*. My name is JT Taylor, and I serve as the Senior Director of Fraud at ID.me. Before this role, I dedicated a significant portion of my professional career to the U.S. Intelligence Community and the U.S. Military, serving in both as an intelligence operations officer. This experience imbued me with a deep understanding of intricate global security dynamics. Later, I served as a Special Agent with the United States Secret Service, where I led a series of pivotal domestic and international fraud and cybercrime investigations. My tenure in intelligence operations and my investigative endeavors have granted me a comprehensive and nuanced perspective on the challenges inherent to digital fraud and cyber threats. As I share insights and recommendations today, drawn from the breadth of my professional journey, I wish to highlight that these views are distinctly my own and may not necessarily align with the official positions of ID.me or affiliated entities.

Historical Context

Before diving into the detailed response mechanisms to the COVID-19 pandemic, it is important to contrast it with a precedent: the 2009 Troubled Asset Relief Program (TARP). Instituted as an emergency measure in response to the financial crisis of 2008-2009, TARP was aimed at stabilizing the crumbling U.S. financial infrastructure, igniting economic growth, and warding off foreclosures that were otherwise preventable.

In October 2008, Congress initially authorized $700 billion for Troubled Asset Relief Program (TARP). However, this amount was subsequently revised and reduced to $475 billion by the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). In contrasting the federal government's response to the 2008 financial crisis with the economic fallout from the COVID-19 pandemic, it becomes evident that each crisis necessitated distinct approaches and oversight mechanisms.

TARP was a significant element of the government's response to the financial crisis of 2008. Recognizing the potential for fraud on such massive amounts of taxpayer dollars, Congress established the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP). With a clear mandate to prevent and detect fraud, waste, and abuse related to the funds appropriated through the Emergency Economic Stabilization Act (EESA) and the Consolidated Appropriations Act of 2016, SIGTARP was positioned as a watchdog.

Armed with the authority to undertake investigations and conduct independent audits, this office was pivotal in ensuring that TARP funds were utilized efficiently, effectively, and in line with Congressional intent.

Fast forward to 2020, and the nation confronted a radically different crisis — a health pandemic with far-reaching economic repercussions. In response, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a stimulus package dwarfing TARP in its magnitude, over four times as large with over $2 trillion earmarked to mitigate the pandemic's economic blow. Notably, the CARES Act did not come with an equivalent to SIGTARP, a singular dedicated oversight body. The absence of a specialized investigative agency specifically tailored for the CARES Act raised concerns about the potential for inefficiencies, fraud, or misuse of the allocated funds.

The differing oversight mechanisms between TARP and the CARES Act underscore the distinct challenges and priorities faced during each crisis. While TARP, conceived in the shadow of banking and financial malfeasance, emphasized stringent oversight to restore public trust, the CARES Act was a rapid response to an unpredictable and evolving pandemic, emphasizing quick dissemination of funds to ensure economic stability. Both responses were shaped by the unique exigencies of their respective moments, and it is evident that the CARES Act would have benefited from a more robust oversight structure akin to SIGTARP.

The CARES Act and Rampant Fraud

The economic challenges posed by the COVID-19 pandemic were unprecedented, demanding a swift and comprehensive response. Whereas TARP was a mechanism to address a financial crisis born out of risky banking practices and mortgage-backed securities, the situation in 2020 was a broad-based public health crisis that spilled over into every facet of the economy. Given the differences in context and scope, the U.S. government's response had to be tailored accordingly.

In March 2020, in reaction to the looming health and economic threats of COVID-19, Congress enacted and the President signed the CARES Act into law, architected with a primary goal: to deliver emergency assistance to the multitudes – both individuals and businesses – battered by the pandemic's repercussions.

In 2022, the Government Accountability Office (GAO) reported that the Federal government made improper payments totaling $247 billion, of which $200 billion were overpayments. This marks a distressing rise from $108 billion in 2012 to $247 billion in 2021.[1]

[1]U. S. Government Accountability Office. Report. Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement. March 29, 2023.

Multiple federal programs continue to hemorrhage taxpayer funds due to these improper payment rates. The COVID-19 pandemic further exacerbated the situation, laying bare significant vulnerabilities in our fraud prevention measures. The vital process of digital identity verification, meant to ensure users – especially those users applying for government benefits online – are genuinely who they claim to be, came under attack. In the initial stages, urgency overshadowed the importance of accuracy and the integrity of the relief programs. Consequently, early initiatives were rolled out without mandating the verification of the claimant. Recognizing this potential weak link, state-level benefits administrators stepped in, enforcing identity verification at diverse stages of the claims process. This insight is pivotal in understanding the backdrop against which my recommendations in this testimony are framed. In the absence of rigorous identity verification for digital government services, the door was left wide open for identity theft and fraudulent claims.

Early into the pandemic, ID.me established a Threat Intelligence Cell (TIC), which unearthed alarming fraudulent tutorials targeting the Small Business Administration (SBA), hosted on platforms like DocMerit and CourseHero. Such threat intelligence is crucial for agencies to fortify defenses, as evidenced by states like California, New York, and Florida, which – among several more – credit ID.me with helping stop approximately $273 billion in unemployment fraud.[2]

However, challenges persist. The latest GAO estimates suggest that unemployment insurance fraud during the pandemic could be between $100 billion and $135 billion.[3] From 2019 to 2020, the Federal Trade Commission saw a staggering 2,920% increase in identity theft reports associated with government document fraud.[4]

Revelations from the Fed ID Forum, backed by findings from both the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Justice, indicate that $212 billion in suspicious 2021 transactions had ties to failures in identity verification.[5] Noteworthy comments from our national security officials equate the scale of this fraud to an economic assault on our nation.

The post-pandemic period still witnesses rampant fraud, challenging our prevention systems. Despite the proven efficacy of the Department of Commerce's National Institute of Standards

[2]State of Arizona Department of Economic Security. "*Arizona Prevents More Than $75 Billion in Unemployment Benefit Fraud.*"; McCarter, Mickey. "*Georgia Sought Identity Verification Solution to Stop Fraud.*" State Tech Magazine, October 13, 2021; State of California, Office of Governor Gavin Newsom. "*EDD Recovers $1.1 Billion in Unemployment Insurance Funds, with More Investigations and Recoveries to Come*" June 21, 2022; Kanowitz, Stephanie. Route Fifty "*UI modernization, identity verification limit state fraud loss.*" March 20, 2023; State of Nevada, Department of Employment, Training and Rehabilitation (DETR). "*Director Elisa Cafferata announces resignation from the Department of Employment, Training and Rehabilitation (DETR)*" December 23, 2022; State of New Jersey, Department of Labor & Workforce Development. "*NJDOL Looks Back at 2021 Accomplishments While Continuing to Aid Workers, Businesses Amid Ongoing Global Pandemic.*" January 3, 2022.
[3] Government Accountability Office (GAO) Report: *More Fraud Has Been Found in Federal COVID Funding—How Much Was Lost Under Unemployment Insurance Programs*. September 13, 2023.
[4]*Federal Trade Commission. 2020 Consumer Sentinel Network Data Book, last accessed, September 24, 2023.*
[5]Martin, Zach. Center for Cybersecurity Policy. *FinCEN: $212 billion in likely financial crimes linked to identity verification breakdowns*. September 13, 2023.

and Technology (NIST) identity assurance standards during the pandemic, some jurisdictions, like Colorado, opted for alternative solutions, resulting in a surge of fraud and innumerable citizens denied their rightful benefits. States such as Ohio and Connecticut are still grappling with fraudulent onslaughts, illustrating the widespread and ongoing nature of this issue.[67] Our nation faces a persistent and multifaceted threat from fraud, and concerted, coordinated efforts are required to address and rectify these vulnerabilities.

The Paycheck Protection Program (PPP)

A noteworthy initiative within the CARES Act was the inception of the Paycheck Protection Program (PPP) in April 2020. Administered by the SBA, the PPP became a lifeline for a spectrum of entities – small businesses, nonprofits, and individuals. The program presented fully guaranteed loans, which were forgivable under specific conditions, enabling businesses to manage payroll costs, including benefits, as well as rent, utilities, and mortgage interest expenses.

Complementing the PPP, the SBA also championed the COVID-19 Economic Injury Disaster Loan (EIDL) program and a related EIDL grant initiative. These were devised to offer a financial cushion to businesses and other organizations grappling with the economic tremors of the pandemic. The EIDL program, in particular, facilitated low-interest, fixed-rate, long-term loans, giving borrowers the crucial working capital to cover routine and essential operational costs.

For perspective, the SBA was entrusted to oversee an unparalleled volume of funds through both the COVID-19 EIDL program and PPP. The deployment was impressive: more than $400 billion was disbursed as COVID-19 EIDL funds, and the PPP scheme saw nearly $800 billion channeled through third-party lending partners.[8]

At the onset of the pandemic, it was evident that the SBA would confront a complex situation: delivering swift relief to Americans in dire need, while also establishing necessary safeguards against the potential for rampant fraud. A predominant concern emerged when the SBA prioritized the rapid distribution of funds to eligible small businesses, potentially overlooking vital internal controls that would reduce the likelihood of fraudulent activity. Such controls include verification processes to ensure that businesses seeking aid genuinely existed before the pandemic and were genuinely impacted by the subsequent economic challenges.

The SBA Office of Inspector General (SBA-OIG), recognizing these challenges, proactively issued two reports even before the first PPP loan was disbursed. In these reports, the emphasis was placed on the necessity of solid, upfront program controls designed to diminish fraud risks.

---

[6] Allen, Jaclyn. Denver7. *Surge in Colorado unemployment fraud affects legitimate claims.* July 25, 2023.
[7] Polansky, Rob. Eyewitness News2. *Labor department suspects 75 percent of unemployment claims are fraudulent* July 21, 2023.
[8] Government Accountability Office (GAO) Report. *Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement* March 29, 2023.

Given the lessons from previous disasters, it was clear that any vulnerabilities in oversight or process, when applied to massive undertakings like the COVID-19 EIDL program and PPP, could lead to significant challenges and potential misuse of funds.[9]

From my vantage point as a then Senior Special Agent for the U.S. Secret Service, when the SBA sought to expedite their disaster loan programs to offer immediate relief, they inherently risked heightening their vulnerability to fraudulent activities and financial losses. The unprecedented surge in loan application volume, fueled by the pandemic, naturally strained their existing oversight mechanisms.

Recognizing this, it became crucial to equip the SBA with insights from previous audits and inspections, especially those that highlighted risks associated with swiftly processing large volumes of loans. To maintain the integrity of these disaster relief programs and reduce the possibility of financial setbacks, it was paramount that the SBA ensured loans were only granted to genuine, eligible applicants. Moreover, the agency needed skilled and adequately trained staff to manage the sheer volume of loans and the urgency surrounding their disbursement.

While the PPP's vast scale and ambition were evident, the SBA-OIG recommended several pivotal measures to curb potential financial losses as loans were rapidly rolled out to qualifying small businesses. This involved instituting strict controls during the loan sanctioning process to rigorously identify participants. The SBA's significant role in navigating the country through the pandemic was unparalleled. Yet, the OIG's anticipatory white paper reports did presage some of the internal challenges the SBA would face in administering the PPP and COVID-19 EIDL initiatives. The SBA managed to facilitate a volume of lending equivalent to 14 years, all within a two-week span. But as the total value of pandemic relief efforts surged past the trillion-dollar mark, it became evident that the SBA preferred a process that was primarily necessitated towards a speedy allocation of funds, inadvertently amplifying risks to taxpayers.

Additionally, some lenders exacerbated fraud vulnerabilities by valuing speed and potential revenue over a meticulous examination of applicant qualifications for governmental support. As an illustration, one particular lender ramped up its loan processing from a mere 200 loans annually to nearly half a million within the pandemic's span, without significantly boosting its workforce or enhancing security protocols.[10] This pursuit of greater profit margins compromised their primary responsibilities, leading to an uptick in identity and eligibility fraud within their loan portfolio. This not only affected taxpayers but also undermined the primary economic objectives of the PPP.

---

[9] U. S. Government Accountability Office. Report. Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement. March 29, 2023.
[10] Ibid.

During the SBA's efforts to respond to the pandemic, the OIG underscored several crucial recommendations to bolster the agency's safeguards against potential fraud, especially concerning the COVID-19 EIDL program and the PPP. The main takeaways from those suggestions are worth highlighting:[11]

- Confirm that loan values don't surpass the stipulated amount per employee.
- Validate that the business was operational before the specified cutoff date.
- They proposed a joint effort with the U.S. Department of the Treasury to create a technical mechanism. This would leverage Treasury's 'Do Not Pay' portal to screen PPP loan applicants, thereby avoiding unwarranted payments and securing federal funds.
- Modify the PPP application to gather borrowers' demographic details.
- Ensuring loans are credited solely to genuine bank accounts of eligible borrowers.
- Prohibiting post-approval alterations to loan application data unless reevaluated by a human reviewer.
- Obtain the applicant's photo ID for identity verification.
- Authenticate the legitimacy of the business using tax records, registration documents, or other relevant means.
- Establish human interactions for applicants with multiple submissions using the same identifiers, like IP or email addresses, to ascertain their authenticity.
- Craft a system that rapidly spots potential risk indicators and necessitates comprehensive mitigation before loan approval.
- Halting any duplicate applications that share identical Employer Identification Numbers (EIN) or Social Security Numbers (SSN).
- Setting up mechanisms that can instantly lock applications with identifiers (like EINs, SSNs, or IP addresses) previously tied to fraudulent activity, ensuring no further malicious submissions.
- Confirming EINs were established prior to the qualifying date for eligibility.

From an outsider's perspective, these recommendations reflect a comprehensive and meticulous approach to ensuring that the SBA's disbursement of critical pandemic-related aid adhered to the highest standards of integrity and accuracy. According to the investigations and data analysis by the SBA-OIG, there appears to be potential fraud exceeding $200 billion associated with the COVID-19 EIDLs and PPP loans.[12]

By harnessing advanced data analytics, past OIG reports, and rigorous investigative techniques, the SBA OIG found that of the funds disbursed, about 17% were potentially fraudulent,

[11] U. S. Government Accountability Office. Report. Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement, March 29, 2023.
[12] Ibid.

comprising over $136 billion from the COVID-19 EIDLs and $64 billion attributed to the PPP loans.[13]

When viewed from a broader perspective, this lapse can be traced back to the SBA's inadequate internal controls in the verification, approval, and disbursement processes. This lack of oversight left the door open for malicious actors, depriving genuine businesses in dire need due to the pandemic's impact from accessing the intended financial support.

To recover a portion of these illicitly acquired funds, investigators must undertake meticulous casework constructed around the digital evidence these wrongdoers inadvertently left behind. These digital breadcrumbs, or "fingerprints," are pivotal in establishing the "Probable Cause to Search." The legal premise of this concept can be elucidated as follows: For the courts to issue a search warrant, they weigh the entirety of the available information to determine whether there's a reasonable likelihood that illegal items, pertinent evidence, or individuals connected to the crime can be located in a specific location.

In observing the actions of the SBA during this crucial period of economic relief, it became clear that there were vulnerabilities in their fraud control mechanisms. SBA-OIG has worked diligently to identify these vulnerabilities and brought several key fraud indicators to light.

As an impartial observer, I would like to share these observations that may guide future investigations:

IP Addresses: SBA-OIG discovered instances where loan applications, under the COVID-19 EIDL and PPP umbrella, were reportedly submitted either from foreign countries or from IP addresses that matched other suspicious applications.

Employer Identification Numbers (EIN): The SBA-OIG found irregularities in the usage of EINs. Some borrowers' EINs either coincided with other PPP loans or were improperly structured, leading to doubts about their authenticity.

Business Establishment Dates: There were cases identified by the SBA-OIG where borrowers claimed their businesses were established after the prescribed cutoff date, suggesting these entities were not eligible for assistance in the first place.

Phone Number Discrepancies: Upon close inspection, the SBA-OIG noted that certain phone numbers were repetitively used across multiple PPP and EIDL applications.

---

[13] U.S. Small Business Administration, Office of Inspector General. Report. *COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape*. June 27, 2023.

Physical Address Irregularities: Similarly, the SBA-OIG flagged numerous instances where applicants used identical physical addresses across a multitude of applications.

Email Address Concerns: The SBA-OIG also highlighted concerns with the use of temporary email domains by applicants, which typically become obsolete after a short span. Furthermore, the crafty use of symbols like dashes and plus signs in email addresses indicated a probable attempt to bypass system checks by managing multiple accounts from a single email.

In reflecting upon the aftermath of the pandemic and the governmental response, one can't help but draw parallels between the vulnerabilities identified in the SBA's loan programs and the challenges faced by the Department of Labor (DOL) and state workforce agencies. As we begin to analyze and comprehend the full spectrum of issues, it's evident that there are shared pain points and lessons to be gleaned.

Interlinked Vulnerabilities: SBA and DOL

The pandemic brought about a monumental shift in global employment patterns, leading to an unparalleled rise in unemployment claims. Many states, faced with rapidly depleting unemployment reserves, found themselves turning to federal loans to ensure the continuation of benefit payouts. Notably, over twenty states took this route, creating a ripple effect that directly burdens the mainstays of our economy: small businesses.

The financing system supporting unemployment benefits is deeply integrated with the broader business ecosystem. Conventionally, businesses make contributions through a tax, calculated based on their workforce size, to support these benefit funds. However, with increasing state debts and evolving economic conditions, this once stable system is now in peril.

States grappling with significant budget deficits have considered reallocating funds initially set aside for mitigating these debts. As a result, the repayment responsibility is gradually being shifted onto businesses. This could mean that businesses, especially small ones, would face progressively increasing per-employee taxes each year for as long as this substantial debt remains—a period some analysts believe could extend up to a decade.[14]

It is worth noting that just a few years ago, certain states reported notable budget surpluses.[15] The failure to utilize these surpluses towards offsetting unemployment debts has resulted in mounting dissatisfaction among business owners. They now confront the financial repercussions of a crisis not of their making, compounded by the fact that many had to shutter operations due to pandemic mandates.

---

[14] Ohanian, Lee. Hoover Institution. (n.d.). *California defaults on $18.5 billion debt, leaving state businesses holding the bag*. April 11, 2023.
[15] Theal, J., & Fleming, J. The Pew Charitable Trusts. *Budget Surpluses Push States' Financial Reserves to All-Time Highs*. May 10, 2022.

Highlighting this situation emphasizes the close-knit relationship between the unemployment benefits system and the health of small businesses. Fraud in unemployment programs doesn't just drain crucial funds; it indirectly threatens the very viability of small businesses, often considered the backbone of our communities. It is essential for policymakers to understand and address this intertwined challenge as Congress deliberates the path ahead.

Both the SBA and the DOL, along with state workforce agencies, encountered an unprecedented surge in the demand for financial relief. With programs like the Pandemic Unemployment Assistance (PUA), Pandemic Emergency Unemployment Compensation (PEUC), and Federal Emergency Unemployment Compensation (FEUC), the disbursement of well over a trillion dollars was no minor feat. While the urgency of the situation necessitated swift action, it inevitably brought to light areas of potential fraud and misuse.

Some common indicators of fraud that emerged in both contexts include questionable IP addresses, duplicative physical and email addresses, and the misuse of identification numbers. Additionally, the sheer volume and velocity of claims and applications made it challenging for these institutions to establish rigorous checks and balances in real-time.

In our eagerness to move beyond the pandemic's hardships, we must be cautious not to overlook the insights these experiences have afforded us. As stewards of public funds and trust, both the SBA and the DOL, together with state entities, have a responsibility to refine their processes, drawing from these lessons. As we prepare for future emergencies, we must prioritize developing more resilient, secure, and efficient systems to ensure that assistance reaches those in need while minimizing the scope for misuse.

Reflecting on the challenges and vulnerabilities of our financial systems, especially in the wake of the pandemic's economic relief programs, it becomes evident that we need robust solutions. Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, Elizabeth Rosenberg, aptly highlighted this in her remarks on January 24, 2022.[16] She observed, *"Rarely in public policy discussions do complex problems have simple solutions... But actually, there really is a kind of a silver bullet, at least one of the closest things to it that I've seen in public policy making–and that's digital ID... digital ID has the potential to immediately and dramatically improve how we protect our national security and our financial security.*

"Indeed, the adoption of such technological solutions can have a transformative effect. We've already witnessed this in action when states like Arizona, realizing the extent of fraud they were subjected to, collaborated with digital ID companies, such as ID.me. The results were profound: the introduction of this digital verification system acted as a deterrent, signaling to the fraudsters that their tactics were no longer viable."

[16] Elizabeth Rosenberg, Assistant Secretary for Terrorist Financing and Financial Crimes, U.S. Treasury. Remarks at Better Identity Coalition. February 1, 2022.

During the tumultuous period of the pandemic, 27 states fortified their cybersecurity defenses by partnering with ID.me for digital identity verification. These states were under siege, facing relentless attacks from both nation-state adversaries and a mix of international and domestic fraudsters armed with vast troves of stolen identities. By integrating with ID.me, these states not only effectively curbed the majority of these fraudulent activities but also expedited the claim processing for genuine applicants. The impact was immense and quantifiable: several states have lauded ID.me for helping to prevent a staggering $273 billion in potential fraud losses.[17] The successful application of NIST standards and robust fraud controls by ID.me played a pivotal role in fortifying security. The SBA's decision not to adopt NIST highlights the potential risks and pitfalls agencies expose themselves to when they don't adhere to the guidelines set forth in OMB M-19-17. It's crucial to underscore the implications of not following these established standards.

Between September 2021 and January 2022, ID.me's Threat Intelligence Cell (TIC) delved deep into the recesses of the dark web to study the prominent players, techniques, and tactics, techniques, and procedures (TTPs) that had targeted the SBA and EIDL loan systems. Their findings illuminated a concerning landscape:

Tutorials Market: The dark web was rife with detailed tutorials on executing fraudulent SBA and EIDL loan applications. These guides meticulously instructed potential fraudsters on the art of using stolen identity data without leaving digital footprints, ensuring a near-seamless theft.

Identity Hunt: A sizeable chunk of the dark web's activity around SBA loans revolved around procuring personal identifying information. The intent was clear: to impersonate genuine businesses and siphon off funds meant for them.

Collaborative Fraud: Many on the dark web sought accomplices for SBA-related fraud. This collaboration hinted at the possibility of multiple players orchestrating large-scale frauds rather than isolated incidents.

Infamous Actors: The dark web had its stars in the world of SBA fraud. Names like Kpoyaga, Krabon Mega, and A stood out, especially as they operated the well-frequented Telegram channel, Kpoyagahack, where they regularly shared insights on exploiting the SBA system. Another noteworthy actor, Ranhacker, had been credited with creating SBA fraud guides that had been spotted on platforms like DocMerit and CourseHero.

[17] State of Arizona Department of Economic Security. "*Arizona Prevents More Than $75 Billion in Unemployment Benefit Fraud.*"; McCarter, Mickey. "*Georgia Sought Identity Verification Solution to Stop Fraud.*" State Tech Magazine, October 13, 2021; State of California, Office of Governor Gavin Newsom. "*EDD Recovers $1.1 Billion in Unemployment Insurance Funds, with More Investigations and Recoveries to Come*" June 21, 2022; Kanowitz, Stephanie. Route Fifty "*UI modernization, identity verification limit state fraud loss.*" March 20, 2023; State of Nevada, Department of Employment, Training and Rehabilitation (DETR). "*Director Elisa Cafferata announces resignation from the Department of Employment, Training and Rehabilitation (DETR)*" December 23, 2022; State of New Jersey, Department of Labor & Workforce Development. "*NJDOL Looks Back at 2021 Accomplishments While Continuing to Aid Workers, Businesses Amid Ongoing Global Pandemic.*" January 3, 2022.

As an observer, it was evident that the dark web had fostered a thriving ecosystem around SBA and EIDL loan fraud, with its actors evolving and adapting swiftly to exploit vulnerabilities. ID.me's TIC has been unrelenting in its dark web surveillance, consistently keeping tabs on nefarious activities targeting the SBA. In its persistent efforts, the cell has recently unearthed dark web posts that elucidate strategies and tactics for defrauding the SBA. The existence of such recent material is indicative of the ongoing threats and underscores the necessity for continuous vigilance and adaptive countermeasures.

A critical oversight by entities like the SBA mirrored the challenges faced by the DOL: they confused identity validation with identity verification. While the former merely ascertains that a combination of a Name, Date of Birth, and Social Security Number is genuine and accurate, the latter dives deeper, ensuring that the individual claiming an identity is indeed the rightful owner of that identity.

The vulnerabilities in relying on identity validation have been brutally exposed due to the plethora of data breaches. An alarming instance was in 2017 when the Chinese People's Liberation Army purportedly pilfered the Equifax database, compromising the sensitive personal information of roughly 150 million American adults. With such an expansive stolen database containing names, dates of birth, and SSNs, malefactors found it easy to deceitfully claim pandemic assistance by simply fabricating their employment records.

A telling account from USA Today highlighted the simplicity of this fraudulent exercise. They interviewed a university student in Africa who candidly shared his modus operandi. By spending just $2 on the dark web, he could purchase stolen identities and file deceptive claims. His strike rate was profitable, managing a successful fraudulent payout for roughly one in every six attempts. His return on investment? A staggering profit, turning an initial outlay of $12 into a fraudulent windfall of $50,000.[18]

The ripples of such activities have a profound human cost. As spotlighted by ProPublica, consider the ordeal of Philip Payton, a violinist for Disney's Frozen musical. Left jobless due to the pandemic, his identity was misused by a criminal to file an unemployment claim in Texas. This fraudulent action triggered a suspension of his genuine unemployment benefits in New York, given the restriction of claiming benefits in one state at a time for specific programs.[19]

The crux of the issue was the inability of these states to distinguish genuine claimants like Mr. Payton from malevolent actors due to inadequate identity verification measures. Tragically, he was left without unemployment benefits from September 2020 to April 2021. His story isn't an isolated incident but echoes the experiences of countless other Americans who suffered similarly.

[18] Penzenstadler, Nick. USA Today. *How scammers siphoned $36B in fraudulent unemployment payments from US. December 30, 2020.*
[19] Hall, Blake. Forbes Technology Council. Council Post. *How Fraud Reduces Access To Benefits.* February 16, 2023.

The widespread and accelerated adoption of the IAL2/AAL2 standard could have served as a robust barrier against the rampant fraud witnessed during the pandemic. Not only would these standards have been instrumental in curbing malicious activities, but they could also have been leveraged to implement enhanced controls to thwart social engineering attempts. Moreover, beyond the obvious advantage of fraud prevention, a uniform embrace of these standards could pave the way for enhanced interoperability across federal and state agencies. This, in turn, would lead to a more streamlined and positive experience for consumers.

Data Brokers Amplify Vulnerabilities: How Third-Party Data Compromises Intensify Fraud in SBA and Federal Benefit Programs

The thriving realm of data brokers has emerged as a potential pitfall in the seamless execution of various state and federal economic relief efforts, particularly in the backdrop of the COVID-19 crisis. Through my research and experiences on this subject, a glaring issue became apparent: hacked accounts from consumer data brokers became potent tools in fraudulent activities. Not only did they aid in bogus COVID-19 related business loans, but also fueled counterfeit unemployment claims.

In mid-2020, renowned cyber-security watchdog KrebsOnSecurity unveiled concerning findings. An informant, seeking anonymity, revealed an alarming trend: a network of fraudsters was rampantly disseminating intricate personal and financial data of Americans.[20] Even more unsettling was the discovery that the data had its roots in a U.S.-based consumer data broker. Investigations unveiled that this analytics giant had been compromised, feeding these fraudsters with invaluable consumer data.

The information trafficked by these scammers is no ordinary data. It encapsulates everything from full Social Security numbers to personal addresses, and even to granular details like IP addresses tied to a consumer's online activities. What made this even more disturbing was the sheer extent and depth of the data being funneled. The compromised data wasn't just aiding identity theft; it was facilitating multi-state unemployment claims and fraudulent loan applications via the SBA.

Historical data serves as a testimony to the recurrent misuse of consumer data. In 2013, a startling revelation saw a 24-year-old operating an identity theft service from Vietnam, granting unauthorized access to the personal and financial data of over 200 million Americans. This breach was orchestrated by deceitfully posing as a private investigator to a subsidiary of Experian – one of the nation's major credit bureaus.[21] Such instances expose the deep-seated vulnerabilities of data brokers and their consequential impact.

---

[20] Krebs, B. KrebsOnSecurity. *Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims. Krebs on Security. August 21, 2020.*

[21] Ibid.

While major credit bureaus remain pivotal, Nicholas Weaver, a distinguished academic from UC Berkeley, suggests that data brokers could be the bigger goldmine for ID thieves. This is primarily because of the breadth and depth of the information they hold, which goes beyond static identifiers like SSNs. It's comprehensive enough for knowledge-based authentication – a primary requirement for credit validations.

Fraudsters typically cash out through money mules, cryptocurrency, prepaid cards, or online-only banks. These instruments allowed for substantial transaction amounts, making them especially attractive for such fraudulent activities.

In light of the revelations brought forth in the speech by the FTC's consumer protection chief, Samuel Levine, it's essential to reassess the expanding footprint of data brokers in the modern digital age. The exponential rise of the data brokerage industry, which amassed a valuation of $240 billion in 2021 and is on track to nearly double by the end of the decade, is not just an economic marvel but poses tangible threats to individual privacy.[22]

Consider this: Data brokers, as Mr. Levine duly noted, wield the power to build intricate profiles about Americans, down to their most private preferences and habits. This power, unchecked and unchallenged, veers dangerously close to infringing upon an individual's right to privacy.[23] In a society where information can be weaponized, do we truly want such intricate details of our lives readily available, often without our explicit consent?

Furthermore, while the industry may justify its practices under the guise of providing customized experiences or streamlining business operations, the undeniable truth remains that individuals rarely have a say in how their data is collected, stored, and shared. Mr. Levine's observations on the industry's "fever" in gathering and selling data are poignant. It's an uncontrolled race where the finish line is unknown, and the implications for individual privacy are extensive.

In a world of increasing transparency, shouldn't we hold data brokers to a similar standard? Levine's call for greater clarity in how companies interact with consumer data is not just sound advice but a foundational principle for safeguarding democratic values. Transparency is not just about business ethics but about protecting the very fabric of our society.

One can't help but concur with Justin Sherman's recent observation to the House Energy and Commerce Committee that the current debate on consumer consent is "broken."[24] The

[22] Lima, Cristiano. The Washington Post. *Analysis | FTC consumer protection chief puts data brokers on notice*. The Washington Post. September 21, 2023.
[23] Ibid.
[24] Sherman, Justin. Testimony. *"Who is Selling Your Data?"* U.S. House of Representatives Energy and Commerce Subcommittee on Oversight and Investigations.

convoluted labyrinth of terms of service agreements, filled with jargon and legalese, effectively ensures that users are unaware of the rights they're signing away. This is not genuine consent but an orchestrated obfuscation of the truth.

Furthermore, while recent FTC actions and penalties against data brokers are commendable, sporadic enforcement is hardly a sustainable solution. The industry's rapid growth, coupled with the complexity of digital ecosystems, necessitates comprehensive and systemic solutions. As FTC Commissioner Rebecca Kelly Slaughter aptly noted, individual enforcement actions can only do so much. It is up to Congress to enact robust, holistic regulations that protect individual privacy rights while ensuring data brokers operate within well-defined, ethical bounds.[25] The era of unchecked data brokerage needs stringent oversight. A balance must be struck between the data-driven digital economy and the inviolable right to privacy. The American people deserve nothing less.

Enhancing SBA's Digital Security & Reclaiming Fraudulent Payments: A Comprehensive Framework

In this testimony, key recommendations are presented to strengthen the Small Business Administration's security framework and enhance its ability to recoup payments that have been mistakenly or fraudulently distributed. Insights from other federal agencies serve as valuable precedents for these suggestions.

1. **Adoption of a Robust Digital Identity Verification System:** Various federal institutions, encompassing the likes of IRS, DOD, and SSA, have successfully integrated digital identity solutions, like ID.me, into their operational framework. These systems, anchored in the guidelines set forth by NIST, equip these agencies with formidable security features. The SBA should likewise integrate such solutions.

2. **Identity Proofing:** It is crucial to ensure that users of public portals are thoroughly verified in alignment with the standards of NIST SP 800-63-3. This guarantees that individuals accessing federal benefits are genuinely who they purport to be.

3. **Empowering User Consent and Control:** Congress should enshrine in legislation the principle that users have the right to granular control over their data. Specifically:

    a. **Granular Consent Mechanisms:** Agencies and businesses should deploy systems that allow users to grant or deny consent for individual uses of their data. This level of specificity empowers users, ensuring they aren't faced with an all-or-nothing choice. For example, users could allow their data to be used for service enhancements but deny its use for commercial advertising.

[25] Lima, Cristiano. The Washington Post. *Analysis | FTC consumer protection chief puts data brokers on notice*. September 21, 2023.

b. **Transparency in Commercial Use:** It's paramount that users are made explicitly aware of any potential commercial (revenue-generating) uses of their data. Clear, concise, and easily accessible disclosures should be provided, outlining exactly how data will be used, by whom, and for what purpose.
c. **Dynamic Control Mechanisms:** Beyond initial consent, users should have the continuous ability to modify their preferences, granting or revoking permissions as they see fit. This dynamic control ensures that consent remains a living choice, adaptable to changing circumstances or user perspectives.
d. **Audit Trails & Accountability:** To bolster trust and compliance, there should be secure audit trails for consent actions. This will serve as a record of what permissions were given, when, and under what conditions. Such trails not only protect users but also provide organizations with a clear record, minimizing potential disputes.
e. **Protection from Coercion:** It's crucial to ensure that users are not penalized or deprived of essential services for refusing to grant consent for commercial use of their data. Consent should be freely given, without fear of negative repercussions.

4. **Prioritizing Security and Data Protection:** The chosen identity solutions should adhere to the standards of FedRAMP Moderate authorization. This commitment ensures the confidentiality, integrity, and overall availability of sensitive data.

5. **Flexibility in Login Options, Maintaining Security:** It is my belief that while fortifying digital defenses, there shouldn't be a compromise on user choice and accessibility. Hence, Congress should consider empowering federal agencies to furnish multiple login alternatives for users. This flexibility should, however, remain within the confines of government-set guidelines. The outcomes of this dual approach not only maximizes access for marginalized groups but also drives down operational expenditures for agencies.

6. **Unified Federal Framework:** Drawing inspiration from countries like Estonia, Sweden, and Norway, where government-issued credentials grant access to various public services, the U.S. should enforce a more harmonized approach. Specifically, the Office of Management and Budget (OMB) Memorandum-19-17 (M-19-17) advocates for a system wherein Americans can choose from either federally or commercially provided shared services, such as ID.me, for identity verification. This model, analogous to the function of digital wallets like PayPal, would facilitate user access while maintaining rigorous security standards.

7. **Reinforced Security Measures:** Evidence suggests that aligning with NIST's Identity Assurance Level 2 (IAL2) standards significantly amplifies the protective measures

against fraudulent activities. For instance, ID.me's adherence to these standards helped save an astounding $273 billion in unemployment funds. Contrarily, deviations from these standards have been met with consequential fraudulent activities.

8. **Strict Adherence and Oversight:** To ensure robust security, the application of the NIST 800-63-3 framework is paramount. This would allow institutions to leverage top-tier cybersecurity knowledge, adapt their protocols as per the risk context, and foster innovation in fraud prevention. A vibrant marketplace already offers Software as a service (SaaS) solutions in line with these standards, ensuring financial institutions remain agile in a dynamically challenging environment. To bolster this, an independent accreditation mechanism should be put in place, steered by an autonomous governance body, distinct from agencies that develop these solutions. This body would ensure conformity, frame performance metrics, and certify providers.

9. **Broadened Data Validation Access:** The Social Security Administration currently offers an electronic Consent Based Social Security Number Verification (eCBSV) tool. This tool, however, is solely accessible to financial institutions. Expanding access to this tool beyond these institutions, especially to approved Credential Service Providers (CSP), would address equity concerns and ensure a wider demographic enjoys unhindered access.

10. **Standardized User Interface Across Portals:** It's pivotal that agencies adopt a uniform user interface for their online platforms, allowing users the liberty to select their identity verification provider and the mode of this verification. Initiated with platforms like Login.gov and ID.me, this would be open to other service providers that adhere to the NIST guidelines and have acquired independent accreditation. Such a standardized interface ensures consumers can elect the most suitable provider for them, reaping the benefits of a competitive landscape.

    To ensure equitable and comprehensive access to public services and benefits, it's imperative that agencies implement versatile identity verification methods, catering to diverse user needs and preferences. These recommendations, derived from the best practices of entities like ID.me, are essential for reaching the entirety of our population, especially the underserved segments.

11. **Flexible Identity Verification Mechanisms:** Agencies must embrace solutions that provide users multiple avenues for identity verification, ensuring no undue burden is placed on the agency or the user. The versatility of these methods ensures that every individual can select a mode that aligns with their comfort and accessibility levels.

a. **Online Self-Service Verification:** This approach allows individuals to independently validate their identity online, typically completing the process in a short span. It's worth noting that a significant majority, approximately 85-90% of users at federal agencies, prefer and utilize this method for its efficiency.

b. **Remote-Assisted Verification via Video Chat:** For individuals whose details might be outdated, missing, or incorrect in credit or public databases, a remote-assisted verification method becomes invaluable.
Here, users can authenticate their identities by interacting with a trained professional through a video call. This method is particularly advantageous for demographics like students with minimal or no credit footprints, recent migrants, or those who've undergone a name change. Evidence from ID.me indicates that this method has successfully verified millions who might have otherwise faced verification barriers.

c. **In-Person Verification Points:** Lastly, a conventional, face-to-face verification method remains pivotal. This allows individuals to confirm their identity at designated physical outlets. With over 680 such retail locations across the nation, it ensures those uncomfortable or unfamiliar with digital means have an accessible alternative.

The integrity of our national services and benefits hinges significantly on the robustness of our identity verification processes. Leveraging established best practices is essential in safeguarding these systems from fraudulent activities and ensuring that genuine beneficiaries have seamless access. Here are my reflections and recommendations on strengthening these mechanisms:

12. **Adherence to NIST's Guidance on Identity Verification:** It's imperative for government agencies to align with the expertly crafted guidelines of the Department of Commerce's National Institute of Standards and Technology (NIST). These guidelines provide a clear roadmap for agencies to assess transactional risks and determine the appropriate identity assurance level (IAL) — ensuring that the level of identity verification rigor matches the potential risks associated with each service or benefit. By utilizing NIST's guidance, agencies can elevate their performance standards and secure their operations against malicious activities.

13. **Opting for NIST Identity Assurance Level 2 (IAL2) Policy**: From ID.me's experience in working alongside federal and state agencies, those that distribute entitlement benefits typically gravitate towards the IAL2 policy. The rationale is grounded in the transaction's inherent risks and the attractiveness of these benefits to potential fraudsters. Some agencies opt for an initial verification process, while others grant users preliminary portal

access with a lower assurance level, subsequently elevating the verification rigor to IAL2 during application initiation. Embracing IAL2 is demonstrably effective in thwarting fraudulent access, thereby ensuring that entitlement benefits reach their rightful beneficiaries.

14. **Establishing Uniformity in Data Retention for Prosecutorial Support:** Currently, the federal landscape is marked by a mosaic of data retention guidelines, with each agency marching to the beat of its own drum. This inconsistency often proves to be a bottleneck in prosecuting fraudulent activities. To overcome this, Congress should champion a standardized approach to data retention, ensuring that all agencies operate under a unified framework. An expert central authority, such as NIST or an alternative governing body, should be entrusted with the responsibility of crafting clear directives on the terms and tenure of data retention. With standardized guidelines, agencies will be better positioned to furnish evidence, bolstering the legal machinery's efforts to hold fraudsters accountable.

Furthermore, it's crucial that each of these verification pathways cater to a multicultural user base by supporting multiple languages. This inclusivity ensures that linguistic barriers don't impede access. Adopting this multifaceted approach to identity verification ensures that no individual, irrespective of their circumstances or preferences, faces undue hindrances when accessing essential services and benefits. In essence, the bedrock of a secure and effective national benefit system lies in both robust identity verification practices and a streamlined approach to data retention. Only by synergizing these elements can we fortify our defenses against fraudulent elements while ensuring that genuine beneficiaries have unhindered access to the services and benefits they are entitled to.

During my examination of the ever-growing digital landscape, ID.me's NIST 800-63-3 IAL2/AAL2 conformant solution has emerged as a powerful tool to both deter fraud and ensure proper identity verification, in ways that simultaneously advance the dual goals of equity and access. This is particularly pertinent in light of the challenges that various populations face, such as communities in Puerto Rico, when trying to access critical online services.

It is worth emphasizing, as pointed out by The Washington Post, that in 2020, less than half of the Americans aiming to set up an online account with the IRS were successful. Former IRS Commissioner Rettig aptly underscored this when he remarked on the IRS's previous system, stating it had a 40% authentication rate. This left 60% of users unable to access services digitally, compelling them to resort to in-person visits or phone calls.Working with ID.me, the IRS was able to get authentication rates well above 70%[26]. This underscores the widespread nature of this challenge and how solutions like ID.me are an absolute necessity in today's digital age.

[26] Singletary, M. Washington Post. *Despite privacy concerns, ID.me nearly doubled the number of people able to create an IRS account.* Washington Post. February 25, 2022.

Puerto Rico's Resident Commissioner to Congress, Jenniffer González-Colón shed light on this concern when gathering insights about the actions the Internal Revenue Service (IRS) was undertaking to enhance its services and accessibility for Puerto Ricans. The encouraging news that followed her inquiry highlighted how new technologies, like those implemented by ID.me, play a pivotal role in bridging these gaps.[27]

Until 2022, a mere 23.9% of Puerto Rican taxpayers could successfully verify their identities online via the IRS Secure Access system.[28] This platform, dependent on data from credit bureaus and data brokers, left a significant portion of the population underserved. However, a paradigm shift occurred when ID.me came into the picture. By integrating with the IRS, ID.me facilitated a range of verification pathways, leading to a staggering rise in Puerto Rican verification success rates to 78.6% – a testament to their efficacy.

This groundbreaking transformation comes at a time when Congress, in a bipartisan effort, scrutinizes the role and practices of data brokers and credit bureaus, especially in the realms of data collection, licensing, selling, and utilization. The evidence is clear: data brokers often falter when it comes to verifying individuals who've experienced recent relocations, name changes, or those who might have minimal credit records. Such shortcomings stress the importance of adopting more innovative solutions from the private sector.

The integration of these state-of-the-art technological solutions has been instrumental in overcoming barriers to access that have long plagued the system. Residents of Puerto Rico deserve seamless authentication, ensuring that they can tap into the critical federal benefits and programs for which they are eligible.

Conclusion

The vast expanse of the digital frontier presents both unprecedented opportunities and challenges. One of the most glaring issues arising from the rapid disbursement of unemployment and small business relief during the pandemic was the loss of hundreds of billions of dollars to fraudulent activities. The sheer magnitude of this loss underscores the vulnerabilities in our current systems and the urgent need for remedial action.

I look forward to discussing the fact that combating these issues cannot solely be a governmental endeavor. There's a palpable need for innovative solutions from the private sector, working symbiotically with governmental efforts, to bring about real, effective change, thwart bad actors, and refine the digital identity experience. The theft of pandemic loan funds showcases the

[27] Congresswoman Jenniffer González-Colón. Press Release. *IRS improves online identity verification for Puerto Ricans in response to rep. Jenniffer González inquiry.* June 8, 2023.
[28] Ibid.

evolving nature of fraudulent activities, and our countermeasures must be equally adaptive, leveraging technology to its full potential.

To Members of Congress and decision-makers alike, the road ahead is clear. Our national interest mandates support for initiatives that underscore technological integration and the harmonization of standards, particularly the NIST 800-63 guidelines. These aren't just bureaucratic checkboxes but essential frameworks that ensure we're always a step ahead of those who seek to exploit the system. Jeremy Grant, the former advisor for the Obama-Biden administration's National Strategy for Trusted Identities in Cyberspace and now Director of the Better Identity Coalition, commented "IAL2 is not just a compliance requirement; in the world of remote identity proofing it is the line between a system that can fend off the bulk of identity theft attacks coming from organized criminals, and one that cannot."[29]

However, the path to recovery and resilience is more than just about stringent measures. It's about fostering an ecosystem of innovation – where our technological capabilities can truly shine in recovering stolen funds and preventing further losses.

Such innovation necessitates continued dialogue and, more importantly, cooperation between the private sector, technological partners, and the government. The synergy from this triad can maximize the efficacy of our recovery efforts and create a robust system, resilient to the multifaceted challenges of the modern era.

In reflection, the trials we've grappled with illuminate the pivotal juncture we stand at today. The American taxpayer, the backbone of our nation, rightfully deserves more. Fortified by collective resilience, forward-thinking strategies, and an unwavering resolve, we're not merely aiming to regain lost ground. We're setting our sights on a future where we craft infrastructures that epitomize security, innovation, and consumer choice. Together, let's chart this ambitious course, driven by our shared aspirations for a more secure tomorrow and our duty to every American taxpayer.

[29] Grant, Jeremy. NextGov/FCW. *Why it's time for a pivot on digital identity.* March 14, 2023.

Testimony of Dean Zerbe

"Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds"
Committee on Small Business, House of Representatives
September 27, 2023

Chairman Williams and Ranking Member Velazquez:

Thank you for the invitation to speak at today's important hearing to explore ways that we can look to private sector solutions to assist in recouping stolen pandemic loan funds – in particular the SBA administered programs of Paycheck Protection Program (PPP) and Covid-19 Economic Injury Disaster Loan (EIDL).

I commend the Committee for wanting to explore new ways to address these concerns of lost taxpayer funds. My testimony will focus on a proven bipartisan way of helping the government uncover fraud and recover taxpayer funds – utilizing and incentivizing whistleblowers to come forward and identify fraud and assist the government in bringing actions against the bad actors.

As the Committee knows, the Small Business Administration (SBA) Inspector General (IG) has reported in its White Paper Report 23-09 "Covid-19 Pandemic EIDL and PPP Loan Fraud Landscape" dated June 27, 2023 ("White Paper") that there has been extensive fraud in these programs. The IG's findings of the loss of taxpayer dollars is supported by the GAO's May 2023 report: "Covid Relief: Fraud Schemes and Indicators in SBA Pandemic Programs. The amount of fraud is certainly eye-blinking – and the Committee is right to want to see if there are new tools that can be utilized in the fight to recover taxpayer funds.

Let me be clear though – I don't consider this a partisan exercise. The efforts to provide Covid relief to small businesses was certainly a well-meaning bipartisan effort. The difficulties of trying to balance the need to quickly move out relief funds and protection of funds were significant – and a challenge to the previous administration and the current administration. It is right, that we look to solutions in a bipartisan manner as well.

Finally, I would note that this problem of significant covid-related fraud is not limited to the SBA. In my work as national managing director of alliantgroup – a nationwide tax services firm – we are helping clients to get right with the IRS and the employee retention credit (ERC). ERC is another covid-related relief program that has unfortunately been subject to a host of pop-up shops hawking snake oil. Our work at alliantgroup, involves either making sure their application for ERC meets all the bells and whistles – and now more and more helping folks clean up inaccurate or incomplete filings made to the IRS because they listened to the siren songs of promoters and filed highly questionable tax refund claims. In short, the problems facing SBA are not unique.

Whistleblower Programs – Tradition of Bipartisan Support

Happily, the solution I discuss today – encouraging and incentivizing whistleblowers – has a long and distinguished bipartisan and bicameral tradition. My former boss Senator Charles Grassley (R-IA) worked hand-in-hand with former Congressman Howard Berman (D-CA) in the 1980s to pass the modernization of the False Claims Act – the grandfather of the whistleblower award programs that has saved taxpayers over $70 billion dollars.

When I served as senior counsel and tax counsel for the Senate Finance Committee, I was the lead staffer for then-Chairman Grassley to pass the 2006 amendments that modernized the IRS whistleblower statute – that has brought in over $6 billion dollars (a number I believe is markedly underestimated). We worked very closely with then-Ranking Member Baucus (D-MT) and his staff on passing these important reforms for the IRS whistleblower program.

Similarly, the SEC and CFTC whistleblower award programs – modeled after the IRS program – all enjoyed bipartisan support.

More recently, Congresswoman Alma Adams (D-NC) and Congressman Anthony Gonzalez (R-OH) successfully sponsored the Anti Money Laundering (AML) Whistleblower Program HR 7195 – which has provided much-needed reform of that whistleblower program.

Bipartisan support for whistleblower award programs has a long tradition – and my hope would be that the Committee would continue that good tradition as it considers similar legislation to create a whistleblower award program for the SBA.

The Benefits of Encouraging Whistleblowers to Come Forward

The GAO report on fraud and the SBA covid-relief programs made the clear point: "Fraud is challenging to detect because of its deceptive nature." (p. 12). That is exactly right – the mischief makers and fraudsters are purposefully hiding and reward laws are key to exposing them.

The National Whistleblower Center (NWC) -- where I serve as a voluntary senior policy advisor -- has done a first-rate job of highlighting major studies showing that whistleblowers are

vital in uncovering and discovering fraud. The NWC highlighted studies include: a 2007 study by PricewaterhouseCoopers *"Economic Crime: people, culture and controls"* found that professional auditors only detected 19% of fraudulent activities at private corporations, while whistleblowers detected and exposed 43%.

A 2006 study from the University of Chicago Booth School of Business, *"Who Blows the Whistle on Corporate Fraud?"* found that employees "clearly have the best access to information. Few, if any, fraud can be committed without the knowledge and often the support of several of them. Some might be accomplices . . .but most are not."

As another NWC paper notes -- the use of reward laws (see National Whistleblower Center: *Importance of Awards*) has been vital in terms of encouraging whistleblowers to come forward – whistleblowers who are often putting much at risk in terms of career and family – and in some cases may face physical threats for doing so. Rewards have been shown to be extremely effective in generating high quality information about fraud that leads to successful prosecutions. (Steve Kohn Executive Director National Whistleblower Center – Testimony December 1, 2016 Before Oversight and Government Reform).

From my own work in tax, I've seen first-hand that the IRS whistleblower award program has been critical in assisting the IRS in dealing with the most difficult areas of tax fraud—especially undeclared overseas accounts by the wealthiest individuals. As I noted in a 2021 Tax Notes article, *"Shrink the Tax Gap by Strengthening the IRS Whistleblower Program"* -- a National Bureau of Economic Research (NBER) paper *"Tax Evasion at the Top of the Income Distribution: Theory and Evidence"* – found that the IRS in expansive individual audits the IRS

was able to uncover undeclared offshore accounts only 7 percent of the time (and these were highly invasive audits

So what did work for the IRS in finding undeclared accounts offshore? Whistleblowers. An academic paper "*Taxing Hidden Wealth: The Consequences of US Enforcement Initiatives on Evasive Foreign Accounts*" (p. 316) – discusses the pivotal role of my client, Bradley Birkenfeld – the UBS whistleblower as breaking open secret Swiss banking. Thanks to Brad coming forward – the U.S. government has recovered billions of dollars from wealthy Americans evading taxes with secret offshore accounts.

Finally, in addition, to the studies and analysis supporting the importance of whistleblowers and incentivizing whistleblowers – the numbers themselves speak volumes. I already spoke of the $70 billion from the False Claims Act and $6 billion from the IRS whistleblower program – but also over $6 billion from the SEC whistleblower program; in 2022 alone the CFTC whistleblower program brought in over $2.2 billion in restitution orders. Clearly, the whistleblower incentives programs are working – identifying fraud that would otherwise go undetected – and as discussed further below – enabling and assisting the work of government.

Deterrent Impact

In addition to helping recover funds, it shouldn't be overlooked how much incentivizing whistleblowers also serves as a significant deterrent effect on fraudsters. In a 2014 Villanova Law Review article, law professor Dennis Ventry (and one-time Chairman of the IRS Advisory Council) -- "*Not Just Whistling Dixie: The Case for Tax Whistleblowers in the States*" – states:

"Whistleblowers can do more than just uncover and report knowing violations of the law. They can also prevent noncompliance from happening in the first place. An effective whistleblower program . . . would add significant risk to noncompliance by increasing the probability of detection and the likelihood of potential penalties, the two most important variables in traditional tax deterrence models."

I have seen this in my own work in tax compliance – where fraudsters are having to calculate not only can they get their snake oil by the IRS – but can they trust everyone involved – the bankers, the secretaries, etc. Similarly, the False Claims Act has had a marked impact in deterring fraud in health care and defense spending (yes, still a ways to go). These industries are well aware of the high risk they face of being exposed for fraud – thanks to whistleblowers. A whistleblower incentive program can not only recover funds – but also serve to put a dampener on future fraud.

Why A Whistleblower Award Program Makes Sense For SBA

Does a whistleblower award program make sense for SBA? Yes. Given the overwhelming amount of fraud and the reality of limited government resources –incentivizing whistleblowers will be an important addition. In short, harnessing the private sector to assist the SBA in its work of recovering taxpayer funds provides an important new tool in combatting fraud.

It is fair to ask whether an SBA whistleblower award program is necessary when whistleblowers can (and have) utilized the False Claims Act (qui tam) to identify and go after

fraud in the SBA covid-relief program. While there has been some use of the False Claims Act to go after PPP fraud in particular – the number of filings has been limited in relation to the amount of fraud. I would note though that those filings have seen success in recovering funds for the taxpayer.

In discussions with practitioners – I believe the limited amount of False Claims Act filings has been due to the fact that the amount of fraud in each individual case is smaller and the potential recovery by the whistleblower is overtaken by the significant costs, time and expense involved in bringing a False Claims Act case. In addition, the proof required in a False Claims Act case, as well as the possibility of the whistleblower being identified all serve to discourage bringing a False Claims Act.

Allowing for both avenues – for a whistleblower to go to the SBA directly or to bring a False Claims Act – is beneficial, giving whistleblowers a choice.

I would underscore that the great benefit of a whistleblower award program is to help the SBA perform its work more effectively and efficiently – and better target the worst actors – saving significant government resources.

In an excellent speech by Andrew Ceresney, Director, Division of Enforcement at the SEC discusses the benefits of the SEC whistleblower program – particularly in terms of fraud: "These [whistleblower] investigations typically involve misconduct that is hard to spot and are typically very document-intensive, involving sophisticated defense counsel. Whistleblowers – particularly company insiders – are able to provide us with a roadmap of the potential

misconduct that can save us months of sifting through documents and complex accounting records. They can also give us a description of the types of documents to request and the types of analyses to conduct."

Similarly, the Treasury Inspector General for Tax Administration (TIGTA) in a 2006 study found (even under the less robust pre-2006 IRS discretionary award program) that "the cost/benefit ration of the [whistleblower] Program compared favorably with other IRS enforcement programs." The report found that the IRS incurred slightly more than 4 cents in costs for each dollar collected from the whistleblower program, compared to a cost of greater than 10 cents per dollar for all enforcement programs.

Further, the TIGTA report found that "examinations initiated based on informant information had a higher dollar yield per hour and a lower no-change rate when compared to returns selected using the IRS' primary method of selecting returns, the Discriminant Index Function [DIF]." The whistleblower-based examinations were found to bring in $946 per hour as opposed to DIF-selected returns that brought in only $548 per hour. Similarly, the no-change rate was only 12 percent for the whistleblower-based audit, while it was 17 percent for DIF-selected audits – finally TIGTA found that whistleblower-based cases brought in $688 per hour compared to $382 per hour for DIF cases.

Most importantly, there was a markedly lower no-change rate for whistleblower-based cases as opposed to DIF cases – meaning that whistleblower selected cases were better at focusing limited IRS resources on the worst actors – and leaving honest taxpayers alone.

In sum, whistleblower award programs are the great friend to honest taxpayers – first, in recovering taxpayer dollars and second, better targeting government enforcement efforts on those individuals seeking to engage in fraud and evasion.

All this speaks to the fact that bringing whistleblowers in to the work of the SBA will help stretch and extend limited existing SBA staff resources – and better focus those resources to be more effective.

SBA IG Embraces Whistleblowers

A key reason that I think a whistleblower program would be a success at the SBA is that the SBA IG, to its credit, already has a good culture when it comes to working with whistleblowers. I was very taken by the strong number of phone calls that the SBA IG in its white paper stated that it has received from whistleblowers already on its hotline – and the number of those whistleblower calls that have led to enforcement action.

The SBA IG white paper highlights that SBA OIG received more than 250,000 calls on its hotline – and that it lead to 90,000 actionable leads. The white paper highlights one case that started out from a hotline complaint as a $500,000 Covid EIDL and PPP fraud involving: "three suspects led us to trace the movement of funds among several co-conspirators'. This ultimately revealed a sprawling conspiracy involving over 1300 non-existent business and up to $140 million in potential fraud. Our data analytics team indicates this one case could further reveal about $625 million in potential fraud." One whistleblower. One case.

Some might say – "well why do an award program – they are coming in already." The reason is that you want more of these high quality cases (many more) and more importantly – by providing an award you are encouraging whistleblowers (who commonly then can bring in counsel – who help improve their filing to be more responsive to the agency's needs and requirements and who also serve essentially as a screener for the agency) to provide a much more robust and detailed filing with the agency.

By bringing in a whistleblower award program that is mandatory – the IRS program changed overnight from being commonly disgruntled prisoners and unhappy former spouses – to senior tax advisors at Fortune 500 companies and bank officers – informed, knowledgeable, insiders – with detailed information and documents. Most importantly – with a whistleblower incentive program you are encouraging whistleblowers and their advisors to spend the necessary time, cost and energy to make a strong filing that is of immediate use to the agency (documents, suggested information/discovery requests, names of additional people to contact, client lists, etc.). The goal of a good whistleblower filing is to – as much as possible – put the fraud on a t-ball for the agency to hit.

Mr. Chairman, as I'm sure you know, the benefits of incentivizing people through a commission or a reward if they meet success is a powerful motivator for hard work and going the extra mile. True for a salesman. True for a whistleblower.

Having a whistleblower incentive program will build on the good foundation of the SBA IG – by encouraging knowledgeable, informed whistleblowers (particularly insiders) to come

forward and for them to file detailed submissions – and as important for the whistleblowers and their advisors to work hand-in-hand with the SBA IG (as needed) going forward.

The SBA IG has a welcoming attitude to whistleblowers – and a culture of openness to whistleblowers. That gives me good confidence of the success of a whistleblower award program at SBA.

The Blueprint For A Good Whistleblower Incentives Bill

As I mentioned in my biography, I was the counsel for the Senate Finance Committee responsible for drafting the IRS whistleblower award program that became law in 2006 – essentially updating, modernizing a whistleblower award program that had been in place since 1867. The 2006 legislation was based largely on the False Claims Act (and the experience of that legislation in practice) – and the IRS whistleblower law served as the model for the SEC, CFTC and other whistleblower award statutes.

What works? What do you need in statute for a whistleblower award program to be successful? A few key points – most of these, if not all are found in the IRS WB bill as well as SEC, CFTC and AML whistleblower bills:

1) Mandatory awards. The whistleblower is not only putting a lot of time, energy and effort into filing – they also may be putting career and livelihood at risk. The whistleblower needs to know that if the SBA uses their information, that the information is material to the government's work and results in funds brought back to the government (or prevention of a payment that otherwise would have been made – protecting revenues) – that the whistleblower will receive an award. That award should

be a percentage (floor and ceiling – commonly 15 – 30%) of the amount returned to the government.

2) The payment of awards should come from proceeds collected thanks to the whistleblower – and should be available and dedicated for that purpose. In short, you want award payments to be a mandatory payment – not subject to appropriations.
3) Create an office at SBA dedicated to engaging with whistleblowers and managing the whistleblower program. Having it within the SBA IG is ideal – given that it will allow the office to work closely with those directly involved with the investigators. The office can also serve as a champion of whistleblowers – to ensure that good cases are being worked and that whistleblowers are being treated fairly and there is good communication with whistleblowers on the status of their submission. Allow the office to publicize awards. Nothing will get whistleblowers to come forward like hearing about other awards. Suggest imposing consideration of a timeline that awards must be made within one year of proceeds collected and rights to appeal by the target have ended.
4) Bad actors – limitations or denials for bad actors. It is well-known that many whistleblowers are not coming from choir practice on their way to the scouts meeting. You are getting (and want to encourage) angels with dirty faces. You want those that are in the room where it happened to blow the whistle. That said, limiting awards for those who planned *and* initiated bad actions and denying an award for those convicted of a crime for the actions they are blowing the whistle is a good balance.
5) Anonymity. While consideration for filing anonymous (but only if have representation – as the SEC does) but regardless, the whistleblower should be protected from his/her

name being disclosed through FOIA or discovery. SBA IG may already have in place such protections given their current active dealings with whistleblowers.

6) Allow for whistleblower to have an independent review. Trust but verify. Whistleblowers will have much greater confidence in the fairness of the program if they are able to receive an independent, de novo review by an outside, separate entity – such as a federal district court. You do not want whistleblower awards to be at the whim of the agency. Independent review gives greater confidence and fairness to the entire whistleblower award program.

7) The proceeds that the government recovers thanks to the whistleblower should be broadly defined to cover all funds recovered (including in related actions) – civil, criminal, disgorgement, etc. The government has wide authority on how it wants to be paid back – how the government gets its money back shouldn't decide the size of the whistleblower's award. Similarly, a whistleblowers value is that their whistleblowing can directly lead to other cases and other recoveries – and the award should be based on the full value the whistleblower has provided.

8) Consider whistleblower protections from retaliation. The Congress recently added 7623(d) to the IRS whistleblower law – and this provides standard language against retaliation to whistleblowers.

9) Consider effective date. While commonly its date of enactment for these matters (information provided after date of enactment) – I would encourage given the desire to be aggressive in combatting fraud – look at having the effective date be today's hearing.

Don't have whistleblowers wait on the sidelines until the provision becomes law. We want them providing information now.

In discussions with Committee staff, I think they have a solid understanding of the framework for a good whistleblower bill and their draft will deserve the Committee's close consideration. I am happy to assist in any way or answer any questions in that good effort.

Conclusion

Mr. Chairman, Ranking Member – thank you for the time and courtesy of allowing me to testify today. I applaud you for considering a whistleblower incentive program as a critical tool to protect the taxpayer. I believe you are very much on the right path.

Testimony of Linda Miller
House Committee on Small Business
Hearing: Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds
September 27, 2023

Summary

The COVID-19 pandemic was the largest and most damaging fraud event in modern history. The two pandemic loan programs administered by the Small Business Administration (SBA)— the Paycheck Protection Program (PPP) and the COVID-19 Economic Injury Disaster Loan program (COVID-EIDL)—were especially targeted by fraud actors. Fraud estimates in these programs vary widely, largely because of differences in definitions and assumptions and a disparity in access to data. While SBA implemented more preventative controls in later rounds of pandemic lending, the backlog of actionable leads of potential fraud in PPP and COVID EIDL to investigate is enormous and the SBA Office of the Inspector General (SBA OIG) is overstretched.

Agencies like the SBA were unprepared for the fraud they encountered largely due to a lack of attention on fraud risks. The Government Accountability Office (GAO) issued its *Framework for Managing Fraud Risks in Federal Programs* in 2015, but regretfully little attention was paid to putting in place the preventative controls to manage fraud risks GAO called for. Congress and the SBA have the opportunity to demonstrate a commitment to preventing fraud in the future, following the devastating fraud losses experienced during the pandemic.

Pandemic Loan Fraud Loss Estimates Vary

In oversight work conducted by the SBA OIG and the GAO, myriad fraud schemes were uncovered in PPP and COVID-EIDL loan programs. For example, fraudsters submitted loan applications using stolen personal and business information and false documentation, such as fabricated payroll records and tax forms. They created fictitious businesses solely for the purpose of obtaining PPP and EIDL loans, with no legitimate operations or employees. In some cases, lenders and borrowers colluded to obtain larger loan amounts or to expedite loan approval, even if the applicant did not meet the eligibility criteria. And due to the urgency of disbursing funds to struggling businesses, there was limited time for thorough verification of applications, which made it easier for fraudulent applications to slip through the cracks.

SBA and the oversight community have different estimates of fraud losses. On the low end, SBA estimates $36 billion of $1.2 trillion (3%) in pandemic relief emergency program funds were obtained fraudulently.[1] On the higher end, SBA OIG estimates that over $200 billion (16.6%) were potentially fraudulent.[2] GAO for its part, identified over 3.7 million unique recipients with fraud indicators out of a total of 13.4 million who applied for SBA pandemic relief programs (27.6%).[3]

---

[1] SBA, *Protecting the Integrity of the Pandemic Relief Programs: SBA's Actions to Prevent, Detect, and Tackle Fraud* (Washington, DC: June 27, 2023).

[2] SBA OIG, *COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape*, Report 23-09 (Washington, DC: June 27, 2023).

[3] GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, DC: May 18, 2023).

At the root of this wide range of estimates are issues related to 1) definitions and assumptions, and 2) data access.

Definitions and Assumptions

The SBA and the OIG have good-faith disagreements about what qualifies a loan as potentially fraudulent. For example, SBA OIG contends that borrowers who fraudulently obtained PPP loans are unlikely to apply for loan forgiveness because they had already obtained the funds and had no intention of repaying or using loan proceeds appropriately. Thus, the OIG includes in its potential fraud estimates all PPP loans in which applicants had not applied for loan forgiveness or made any required principal repayments as of May 2023, resulting in borrower default of the loan.

In contrast, SBA contends that many defaulted loans are not fraudulent; they represent real businesses that did not make it through the turbulence of the pandemic, have no ability to repay, and no longer exist to apply for loan forgiveness, or are simply not aware this is an option.

Likewise, according to SBA, 88% of COVID-EIDL lending went to businesses that have either fully repaid their loan or begun to do so (74%) or are still in the allowed deferment period (14%). According to SBA, common sense dictates that a bad actor would not fraudulently obtain a loan, only to repay it with interest. OIG, on the other hand, believes that repayment alone is not a factor in whether the underlying application was potentially fraudulent.

The truth most likely lies somewhere in the middle.

These differences in opinion demonstrate the value of using common definitions when measuring and estimating fraud. Consistent definitions would allow experts to compare and aggregate data within and across agencies, assess trends, and show progress in fraud prevention.

Data Access

Another key reason there are differing estimates of fraud is that SBA cannot access datasets that the OIG and GAO can. For example, the GAO analyzed PPP data using comparisons against the National Directory of New Hires (NDNH) wage data at the Department of Health and Human Services (HHS), whereas SBA cannot access these datasets.

Furthermore, SBA was initially barred from using IRS data to check for identity fraud. After Congress granted SBA the authority in 2021 to use IRS data to verify identity for its pandemic programs, it was able to make improvements in its processes for identifying and denying loans to ineligible and fraudulent applicants.

Improving agency access to data is a key accelerator in fraud prevention and detection. For instance, in January 2023, the PRAC urged SBA to work with the Social Security Administration (SSA) to explore information-sharing agreements that will allow for verifications across all SBA-funded grant, loan, and benefit programs that are vulnerable to identity fraud.[4] SBA concurred and has coordinated with SSA on this matter, but as of April 2023, the SBA found that SSA may lack the legal authority to share information with SBA.

I have long advocated for better data access, sharing and analytics in preventing and detecting fraud. Agencies cannot prevent fraud if they cannot access the data needed to detect it in the first place. And even today, three and a half years after the pandemic started, Treasury's Do Not Pay

[4] PRAC, *FRAUD ALERT: PRAC Identifies $5.4 Billion in Potentially Fraudulent Pandemic Loans Obtained Using Over 69,000 Questionable Social Security Numbers* (Washington, DC: January 30, 2023).

system continues to lack access to SSA's full death data and it may be cost-prohibitive for Treasury to purchase it.

I have previously recommended that Congress establish a well-funded, centralized antifraud office that would have the necessary skills and focus to work on addressing the profound data challenges facing every level of government when it comes to preventing fraud. It is imperative that Congress learn from the lessons the pandemic provided by helping to facilitate better access to and sharing of data.

Preventative Controls Save Taxpayer Money

As in medicine, so in fraud: Prevention is key. Every dollar invested in fraud risk management can result in thousands, if not millions, of dollars saved. Both GAO and OMB have issued guidance noting that preventive controls are more effective than a "pay-and-chase" model.

SBA has seen this firsthand. After it began implementing improved internal controls and data screening practices midway through the pandemic—such as pre-award application screenings, automated screenings for PPP, tax transcript verifications for COVID-EIDL, and data checks using the Treasury Department's Do Not Pay system—the agency observed substantial savings in prevented fraud. Thanks to these improvements, SBA estimates that it achieved dramatically lower fraud rates in the two relief programs designed and launched in 2021, Shuttered Venue Operators Grants (SVOG) and the Restaurant Revitalization Fund (RRF). SBA must further invest in advanced analytics and improve its use of intra-agency data to identify fraud indicators in its loan programs going forward, and Congress should ensure SBA is resourced to do so.

Identity Theft Poses a Significant Threat

Identity theft has emerged as the largest fraud threat facing organizations today. The massive trove of personally identifiable information available for sale through data breaches coupled with advanced technology like deepfakes— accelerated by Generative AI voice spoofing— create a significant risk to government programs. The pandemic created the means for fraud actors to steal at scale using stolen identities.

It is unknown how much of the PPP and EIDL fraud was identity theft-related, but some indicators reveal that it may have been significant. In August 2021, the OIG reported over 1 million complaints of EIDL loan identity theft. In January 2023 the PRAC identified over 221,000 Social Security Numbers (SSNs) used on applications that were either not issued by SSA or that identifying information in SSA's records did not match the name and/or date of birth information provided by the COVID-19 EIDL or PPP applicant, suggesting potential identity fraud in the use of those SSNs. The PRAC also determined that $5.4 billion in COVID-19 EIDL or PPP loans was disbursed to applicants using 69,323 of those SSNs between April 2020 and October 2022.

SBA has implemented some controls that can screen for the presence of stolen identities since the start of the pandemic. It is vital that the fraud risk management efforts the agency undertakes going forward include robust tools to uncover possible identity theft before approving a loan. SBA leadership must demonstrate sustained attention and commitment to fight this new, more sophisticated adversary.

Investigations Backlog is Enormous, and the OIG is Overstretched

The vast majority of the pandemic loan programs are now over, and in the case of PPP, the forgiven loans have largely been extinguished, leaving the work of clawing back fraudulent funds to the OIG and its law enforcement partners.

Investigations yield a substantial return on investment. In 2019, SBA OIG achieved $111.0 million in monetary recoveries and savings—a fivefold return on investment to the taxpayers, and in 2020, OIG achieved $142.5 million in monetary recoveries and savings—a sixfold return on investment to the taxpayer.[5]

Yet, the SBA OIG remains woefully under resourced when compared to the challenge it faces. SBA has referred or likely will refer 744,000 cases of likely fraud from approved awards, grants, and loans to its OIG. The OIG has repeatedly and publicly indicated that the office is overstretched. Deputy IG Shoemaker told Congress in March 2023 that the office had over 80,000 actionable leads, but only 550 open cases across both PPP and COVID-EIDL.[6] SBA describes the analytic process it undertook to get to $36 billion in suspicious loans that it then referred to OIG as comprehensive and believes that its analysis provides a basis for the OIG to focus its investigative resources on those loans.

SBA's COVID-19 programs were three times the size of the 2009 Troubled Asset Relief Program (TARP) and significantly more complex, but SBA OIG's funding has been significantly less than the funding Congress provided for TARP. In the FY 2023 Omnibus passed in December 2022, Congress provided $32 million to SBA OIG. However, more resources for law enforcement are needed. Continued increases in annual appropriations for OIG will enable the office to enhance its data analytics unit and hire more permanent investigative personnel.

Conclusions

Lessons from the pandemic are already being applied at SBA. GAO has made recommendations to the SBA to enhance its proactive fraud risk management posture and in response, the agency has made progress in implementing a more robust framework, including establishing a Fraud Risk Management Board as a designated entity, in accordance with the GAO Fraud Risk Management Framework.

More work remains. Through proactively and regularly assessing vulnerabilities in its programs, implementing data-driven, preventative controls, establishing a culture where staff feel comfortable talking about fraud, and collaboratively engaging with the OIG, SBA can help ensure that it is well-prepared for any future crises that may be exploited by fraud actors. Congress can play a role by helping facilitate access to datasets and providing funding to the OIG to address its investigative backlog and to SBA to implement advanced, data-driven fraud prevention tools.

[5] SBA OIG, *FY 2022 Congressional Budget Justification* (Washington, DC: May 2021).

[6] SBA, *Protecting the Integrity of the Pandemic Relief Programs.*

Questions for the Record
Full Committee Hearing: Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds.
Small Business Committee
September 27, 2023

Ms. Linda Miller, Former Deputy Executive Director, Pandemic Response Accountability Committee (PRAC)

- The oversight and law enforcement agencies have begun to use advanced data analytics, which offer a number of ways to analyze and interpret data to prevent and recoup fraudulent funds. Could you discuss the effectiveness of this new tool, and how it may help the OIG to recoup some of the potentially fraudulent funds?

Advanced analytics tools include machine learning/artificial intelligence capabilities that can identify patterns that indicate potential fraud in loan applications or in borrower activity post origination. For example, anomaly detection can be used to identify the total time a financial institution spent conducting due diligence relative to the average timeframe across all loan applications to identify those applications with unusually short due diligence time periods. Similarly, techniques such as graph or network analytics can be used to identify relationships among borrowers or between borrowers and individuals with known criminal histories to identify suspicious applicants associated with known criminals. SBA and the SBA OIG can also use third party data to identify identity-theft related fraud, such as mismatches between identifying information associated with individuals, by matching applicant provided information with public records data. The SBA OIG has made use of many such tools to identify potential fraud in pandemic loans, in some cases in partnership with the Pandemic Analytics Center of Excellence (PACE).

- We have heard testimony today that SBA should integrate digital identity solutions like ID.me into its current systems, could you assess this recommendation and share with the Committee your perspective on how effective this proposal would be in mitigating fraud at SBA?

Federal agencies have available to them several digital identity technology solutions that can be valuable for use in authenticating users. I believe it's important to remain vendor-agnostic when choosing such tools and to adhere to established procurement processes to evaluate the effectiveness and cost of different options before choosing a vendor. Going forward, SBA should conduct a thorough fraud risk assessment of its loan programs and make the determination of whether to acquire a digital identity verification solution independently, evaluating vendors for value and effectiveness. Its important to recognize that no tool is a panacea and the right mix of technology will vary depending on the fraud risk the agency faces. Digital identity verification tools have more applicability in certain federal programs than others and private sector companies have financial incentives for advocating the use of their tools. Thus, every agency should apply a rigorous process when evaluating the merits of different types of technologies to procure, based on their risk profile.

- Could you please share with the Committee any innovative ideas that would enable the Federal government to recoup potentially fraudulent funds?

SBA could consider providing amnesty to PPP and COVID EIDL recipients who come forward voluntarily and offer to return the funds they obtained through means, either intentionally or unintentionally, that were improper. I believe there are many borrowers who may understand they improperly received COVID EIDL or PPP loans but are not coming forward because they fear criminal or civil penalties. If the goal is to recoup improperly paid out funds, the focus should be facilitating the return of those funds, rather than on penalizing people, which is likely disincentivizing some proportion of borrowers from voluntarily returning the funds.

[DISCUSSION DRAFT]

118TH CONGRESS
1ST SESSION

H. R. _____

To amend the Small Business Act to establish the Office of Whistleblower Awards, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Small Business Act to establish the Office of Whistleblower Awards, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Put America on Commission Act of 2023".

SEC. 2. ESTABLISHMENT OF THE OFFICE OF WHISTLEBLOWER AWARDS.

The Small Business Act (15 U.S.C. 631 et seq.) is amended—

(1) by redesignating section 49 as section 50; and

(2) by inserting after section 48 the following new section:".

"SEC. 49. OFFICE OF WHISTLEBLOWER AWARDS.

"(a) ESTABLISHMENT.—There is established within the Office of the Inspector General of the Small Business Administration an Office of Whistleblower Awards.

"(b) ADMINISTRATION.—The Office of Whistleblower Awards shall be administered by an Assistant Administrator, who shall be an employee in the competitive service.

"(c) DUTIES.—The Assistant Administrator shall—

"(1) make recommendations to the Inspector General relating to making awards to whistleblowers as described in subsection (d)(1); and

"(2) determining the amount of such awards as described in subsection (d)(2).

"(d) AWARDS TO WHISTLEBLOWERS.—

"(1) IN GENERAL.—The Inspector General, upon recommendation from the Assistant Administrator, may pay amounts as described in paragraph (2) to a whistleblower for information relating to financial misconduct or fraudulent misrepresentation by a recipient of financial assistance from the Administrator, if—

"(A) the Inspector General commences an investigation, or takes administrative or judicial action relating to information; and

"(B) the action taken by the Inspector General results in monetary recovery.

"(2) AMOUNTS.—Any amount payable under this section shall be paid from the proceeds of any amounts collected by the Inspector General as a result of an administrative or judicial action relating to information provided by the whistleblower as follows:

"(A) The whistleblower shall, subject to subparagraph (B), receive not less than 15 percent but not more than 30 percent of the proceeds (including penalties, interest, and additional amounts) resulting from such action (including any related actions) or from any settlement in response to such action (or such related action).

"(B) If such information did not result in the initiation of such action, and if the Assistant Administrator determines such action is based principally on disclosures of specific allegations (other than information provided by the whistleblower) resulting from another judicial

or administrative hearing, from a government report, hearing, audit, or investigation, or from the news media, the Assistant Administrator may award not more than 10 percent of the proceeds (including penalties, interest, and additional amounts) resulting from the action (including any related actions) or from any settlement in response to such action.

"(e) DISCRETION.—The Assistant Administrator shall determine the percentage of proceeds a whistleblower receives as an award under subsection (d) based on—

"(1) the significance of the information provided by the whistleblower to the action described in such subsection;

"(2) the extent to which the whistleblower contributed to the action described in such subsection; and

"(3) for the purposes of determining an award under subsection (d)(2)(B), the extent to which any legal representative of the whistleblower contributed to such action.

"(f) ADDITIONAL REQUIREMENTS.—

"(1) REDUCTION IN AWARD.—If the Assistant Administrator determines that the whistleblower who provided the information also planned or initiated

the actions that led to the to financial misconduct or fraudulent misrepresentation by a recipient of financial assistance from the Administrator, the Assistant Administrator may reduce such award.

"(2) REPAYMENT.—As a condition of receiving an award under this section, the whistleblower shall agree to repay the full amount of the award if the whistleblower is convicted of a crime relating to the information that was the basis for receipt of such award.

"(3) NO CONTRACT NECESSARY.—A whistleblower shall not be required to be a party to a contract with the Office of the Inspector General of the Small Business Administration to be eligible to receive an award under this section.

"(g) APPEALS.—A determination made under this section by the Assistant Administrator, except the determination of the amount of an award if the award was made in accordance with the requirements of subsection (d)(2), may be appealed by the whistleblower subject to such determination to [the appropriate court of appeals of the United States] not more than 30 days after the determination is issued by the Assistant Administrator. [The court] shall review the determination in accordance with section 706 of title 5, United States Code.

"(h) GUIDANCE.—Not later than four months after the date of the enactment of this section, the Administrator shall issue guidance to carry out the requirements of this section.

"(i) REPORT.—Not later than 12 months after the date of the enactment of this section and annually thereafter, the Inspector General shall submit to Congress a report on—

"(1) the number of times whistleblowers submit information to the Inspector General;

"(2) the amount of awards disbursed under this section; and

"(3) any legislative or administrative recommendations regarding the duties of the Office of Whistleblower Awards.

"(j) DEFINITIONS.—In this section:

"(1) ASSISTANT ADMINISTRATOR.—The term 'Assistant Administrator' means the Assistant Administrator of the Whistleblower Awards Office.

"(2) INSPECTOR GENERAL.—The term 'Inspector General' means the Inspector General of the Small Business Administration.

"(3) PROCEEDS.—The term 'proceeds' means—

"(A) penalties, interest, and additional amounts collected in an administrative or judi-

cial action (or related action) taken by the Inspector General relating to information provided by a whistleblower under this section; and

"(B) any amount collected by Administrator or the Inspector General pursuant to the administrative, enforcement, or investigative authority of the Administrator and the Inspector General, respectively, including—

"(i) criminal fines and civil forfeitures; and

"(ii) amounts collected for violations of reporting requirements.

"(4) WHISTLEBLOWER.—The term 'whistleblower' means an individual who is aware of a violation of any law, rule, or regulation relating to financial misconduct or fraudulent misrepresentation by a recipient of financial assistance from the Administrator.".